Over 8,600 Vulnerabilities Found in Pacemakers

Over 8,600 Vulnerabilities Found in Pacemakers

Millions of people that rely on pacemakers to keep their hearts beating are at risk of software glitches and hackers, which could eventually take their lives. A pacemaker is a small electrical battery-operated device that's surgically implanted in the chest to help control the heartbeats.…[Lire la suite]

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 sur cette page.

Réagissez à cet article

Alerte : Mettez à jour votre Google Chrome

Alerte : Mettez à jour votre Google Chrome

Sur Windows, MacOs et Linux, de multiples vulnérabilités dans Google Chrome ont été détectées par le CERT (Computer Emergency Reponse Team) de l'ANSSI (Agence nationale de la sécurité des systèmes d'information).

Systèmes affectés

Chrome versions antérieures à 59.0.3071.86 pour Windows, Mac et Linux

Résumé

De multiples vulnérabilités ont été corrigées dans Google Chrome. Elles permettent à un attaquant de provoquer un problème de sécurité non spécifié par l'éditeur et un contournement de la politique de sécurité.

Comment mettre à jour ?

Cliquez sur les 3 points verticaux (en haut à droite du navigateur), descendez la souris sur « Aide » et cliquez sur « À propos de Google Chrome » et sur « Mise à jour ».
Sinon, vous pouvez aussi télécharger la dernière version de Google Chrome sur « https://www.google.fr/chrome/browser/desktop/index.html »
[Plus d'infos ici]

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 d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Réagissez à cet article

Source : *Multiples vulnérabilités dans Google Chrome*

Votre voix pour remplacer vos mots de passe

	Votre voix pour remplacer vos mots de passe

La Banque Postale est la première institution à avoir obtenu l'autorisation de la Commission nationale informatique et libertés (CNIL) pour tester en France une technologie évaluant la voix de ses clients pour leur permettre de se connecter à leur compte en ligne.

La Banque postale inscrit son innovation dans un nouveau service de paiement en ligne baptisé « Talk to Pay » (littéralement « parler pour payer »). Un dispositif qui se rapproche de l'outil mis en ligne pendant l'été 2016 par MasterCard, qui permet de confirmer un paiement en ligne grâce à la reconnaissance faciale.
[lire la suite]

Commentaire de Denis JACOPINI :
Un pas de plus vers la biométrie qui, comme les objets connectés, peut nous faire vivre certes dans un monde connecté mais également dans un monde piraté.
Du jour au lendemain nos informations biométriques (empreintes, iris, voix…) peuvent se retrouver piratées et recopiés sans compter que la voix peut changer avec le temps et avec les saisons (rhume, allergie,).

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 d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Réagissez à cet article

Source : *Cybersécurité : les 6 techniques qui pourraient remplacer le mot de passe*

Quels sont avantages à se

mettre en règle avec le RGPD ?

	Quels sont les avantages à se mettre en règle avec le RGPD?

Avec le Règlement Général sur la Protection des Données (RGPD/GDPR), l'UE se dote d'un cadre réglementaire détaillé pour permettre à ses citoyens de reprendre le contrôle sur leurs données numériques. Pour se mettre en conformité, les entreprises ont un travail titanesque devant elles pour ne pas risquer de lourdes amandes prévues par le texte. Quels avantages peuvent tirer les entreprises de prendre le chemin de la mise en conformité ?

Au fil des conférences que nous animons ou des réunions de sensibilisations auxquelles il nous est demandé d'intervenir, nous remarquons que la grande majorité des décideurs voient d'un très mauvais oeil l'arrive de ce RGPD (Règlement Général sur la Protection des Données).

Le contexte

A cela, Denis JACOPINI, Expert Informatique spécialisé en protection des données personnelles répond plusieurs choses :

1. Ne pensez-vous pas qu'en tant que consommateur, vous êtes en droit d'avoir l'assurance que le professionnel ou le service public à qui vous confiez vos données personnelles (adresse postale, adresse e-mail, date de naissance, n° de tel portable, numéro de carte bancaire, numéro de sécurité sociale, mot de passe pour accéder à notre compte, historique et remboursement de nos actes médicaux, empreintes digitales, vocales, iriennes, adn, photocopie de pièce d'identité ou de justificatif de domicile…) mettra tous les moyens techniques en oeuvre pour protéger votre vie privée ?

A l'heure de la communication de nos données à la vitesse de la lumières peut encore penser que toutes les données nous concernant, absolument toutes, doivent être libres d'accès ?

Ceux qui ne craignent pas les usages malveillants de ces données ?

A mon avis ce sont ceux qui ne connaissent pas les conséquences d'une usurpation d'identité, d'un vol de numéro de carte bancaire ou d'un vol de mot de passe.

2. Denis JACOPINI vous demande maintenant de vous positionner à la place du responsable de l'établissement public ou privé qui a maintenant la lourde responsabilité de conserver et protéger toutes les informations que lu ont confié des milliers voire des millions de personnes.

Maintenant, n'est-il pas normal de faire le ménage dans votre système de traitement de données et de supprimer ou d'anonymiser les données inutiles ?

Ne pensez-vous pas qu'il est important de mettre à l'abris des regards indiscrets les numéros de cartes bancaires que vous avez récupéré dans votre système informatique ou bien plus couramment sur les tickets de votre TPE ?

Ne pensez-vous pas que les SEULES données pour lesquelles pour vous TOUT est permis ce sont VOS DONNÉES (votre nom, votre prénom, votre date de naissance, vos numéros de téléphone, nos numéro de CB, vos mots de passe, les chiffres de votre comptabilité…). ous pouvez faire ce que vous voulez avec VOS données (les accrocher derrière un Sessna et les faire défiler dans le ciel si ça vous chante). Toutes les autres données, celle appartenant à d'autres personnes ne vous appartiennent pas et vous ne pouvez pas faire ce que vous voulez avec.

Toutes les autres données appartiennent à des personnes qui comptent, et cela va de sois, sur votre discrétion et votre professionnalisme pour ne pas diffuser, divulguer ou rendre accessible ces données à des tiers non autorisés ou malveillants.

3. A l'heure des gros titres quasiment quotidiens faisant état d'un usage de données volées, de la diffusion ou de la vente dans le « darknet » (sorte de marché noir de l'Internet) ou pire, dans l'Internet public de données volées à des personnes comme vous et moi, il est, selon l'avis de Denis JACOPINI urgent d'arrêter de donner à manger à ces pirates informatiques qui basent avant tout leur activité lucratives sur les erreurs et failles des utilisateurs et informaticiens négligents insensibles à la sécurité informatique ne se souciant que de la part disponibilité ou intégrité dans leur applications de la sécurité informatiques, mais ni de confidentialité et encore moins d'analyse de risque.

Les opportunités pour les établissements concernés

En entamant une démarche de mise en conformité avec la Loi Informatique et liberté I ou II, avec la Loi pour une République Numérique ou avec le RGPD (Réglement Général sur la Protection des Données), Denis JACOPINI ajoute que vous allez être amenés à corriger plusieurs failles dans les traitements de données personnelles dont votre activité administrative ou professionnelles dépend :

• En vous intéressant à la durée de conservation de vos documents, vous allez épurer vos archives contenant la plupart du temps « au cas où » la totalité de la mémoire de l'entreprise de la plus petite notre manuscrite jusqu'au dossier complet sur une entreprise ou une personne en particulier. En mettant à plat l'ensemble de vos traitements de données personnelles, vous constaterez très certainement que vous conservez des données sans y être obligé. Les détruire vous permettra non seulement de gagner de la place **(Gain de place = Gain d'argent)**, mais également de réduire vos responsabilité en sécurisant l'accès à ces données confidentielles pour la plupart **(Moins de responsabilités = moins de risque)** ;

• Concernant la confidentialité, vous allez ensuite vous rendre compte qu'à la question QUI à accès à QUOI ? il est peut être temps de faire du ménage. Entre les utilisateurs qui n'existent plus et les dossiers contenant des informations sensibles partagés sans restriction particulière, il sera probablement nécessaire de revoir sa PSSI (Politique de Sécurité des Systèmes d'Information) ; L'entreprise y tirera un avantage en matière de tranquillité et surtout cela diminuera ses responsabilités en cas de vol de données **(Moins de risques = Plus de tranquillité)** ;

• Difficile de mettre en place une telle démarche sans avoir une personne dédiée à ces fonctions. Jusqu'au 25 mais 2018 il s'appelle CIL (Correspondant Informatique et Libertés) et DPO (Data Protection Officer) ensuite. Ce soldat dédié à la protection des données n'est pas là que pour dire à son employeur ce qu'il faut faire pour rester dans les clous de la réglementation sur les données personnelles ou signaler ce qu'il ne faut pas faire.

Cette personne dédiée à temps partiel ou à temps complet à ces fonctions a pour but, par son existence et sa déclaration auprès de l'autorité compétente (la CNIL en France), de rassurer celui qui vous a confié, qui vous confie et qui vous confiera encore des données personnelles. Sachant que bientôt la quasi totalité des citoyens et consommateurs déposeront des informations auprès d'organismes ou sur des site Internet essentiellement parce qu'ils ont confiance envers le service utilisé, l'existence de cet intermédiaire entre l'autorité compétente et votre établissement sera à minima essentielle pour ne pas faire fuir les usagers de vos services **(Plus de confiance = Plus d'activité)**.

Autres avantages collatéraux

En entamant une démarche de mise en conformité avec les lois relatives à la protection des données personnelles, vous contribuez à la diminution de la cybercriminalité dans le monde. En effet, données plus protégées = données difficile à voler par les pirates du Web = moins de pirates = moins de temps perdu à traiter les prélèvements frauduleux, les usurpations d'identité et pannes informatiques.

Les démarches à accomplir recommandées par Denis JACOPINI

1. Faire un état des lieux des données personnelles soumises à la réglementation ;
2. Rechercher la présence ou non de dérogation ou d'exception relatives à votre activité ou aux données personnelles traitées ;
3. Réaliser une analyse de risque relative aux données personnelles (Denis JACOPINI a spécialement passé la certification ISO 27005 qui concerne les analyses de risques relatives aux données) ;
4. Mettre en conformité les traitements des données personnelles afin qu'ils répondent aux réglementations (Loi Informatique et Libertés / Loi pour une République Numérique / Règlement Général sur la Protection des Données RGPD) ;
5. Mettre en place un registre et porter les annotations nécessaires à l'amélioration des traitements ;
6. Suivre l'évolution de l'établissement, des traitements, des risques et mettre à jour le registre.

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 d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Réagissez à cet article

Un DSI laisse des backdoors pour pirater son ancien employeur

Un DSI laisse des backdoors pour pirater son ancien employeur

Un ancien responsable IT de Columbia Sportswear a laissé 2 backdoors pour récupérer des documents commerciaux utiles à son nouvel employeur.

En matière de sécurité informatique, la menace n'est pas uniquement à l'extérieur de l'entreprise, mais aussi à l'intérieur. Columbia Sportswear, fabricant de vêtements de sports, vient d'en faire l'amère expérience.
En effet, la Cour de l'Oregon va être amené à se prononcer sur une affaire concernant Michael Leeper, ancien DSI de Columbia Sportswear. Il est accusé de vol de données confidentielles au bénéfice d'un partenaire commercial.
Petit rappel historique, Michael Leeper a démarré sa carrière chez Columbia en 2000, comme responsable de l'équipe en charge des PC. Il obtient des promotions pour atteindre le poste de directeur des infrastructures technologiques où il est en charge de la maintenance du système d'information de Columbia et de signer les contrats avec les fournisseurs technologiques. Il était en contact notamment avec Denali, un fournisseur qu'il a rejoint en 2014.

Rester dans le réseau de manière masquée

Mais, juste avant de partir, le responsable IT se serait créé un compte réseau sous le nom « Jeff Maning », aussi appelé « jmanning ». Ce qui lui aurait permis d'accéder au réseau de Columbia, y compris via le VPN et le VDI de la société. Un accès utilisé plus de 700 fois par Michael Leeper pendant 2 ans, afin de voler des documents sensibles de Columbia (plan d'affaires, budget IT, etc) au profit de Denali selon l'accusation. Il aurait mis en place une seconde backdoor (« svcmon ») liée à un compte utilisé par les administrateurs systèmes pour surveiller l'activité réseau. Avant de partir, Michael Leeper s'y serait octroyé le privilège maximal.
Dans sa plainte, Columbia estime que Michael Leeper a eu accès à des e-mails sur des accords commerciaux dans lesquels Denali avait des intérêts financiers. Le prestataire s'est défendu dans un communiqué en indiquant qu'une telle affaire « *ne reflète nullement la politique de Denali et ses valeurs* ». La société précise coopérer à l'enquête et a donné congé à son CTO, Michael Leeper, afin, officiellement, qu'il puisse organiser sereinement sa défense…[lire la suite]

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 d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Réagissez à cet article

Source : *Quand un DSI laisse des backdoors pour pirater son ancien employeur*

Un DSI laisse des backdoors pour pirater son ancien employeur

Un DSI laisse des backdoors pour pirater son ancien employeur

Un ancien responsable IT de Columbia Sportswear a laissé 2 backdoors pour récupérer des documents commerciaux utiles à son nouvel employeur.

En matière de sécurité informatique, la menace n'est pas uniquement à l'extérieur de l'entreprise, mais aussi à l'intérieur. Columbia Sportswear, fabricant de vêtements de sports, vient d'en faire l'amère expérience.
En effet, la Cour de l'Oregon va être amené à se prononcer sur une affaire concernant Michael Leeper, ancien DSI de Columbia Sportswear. Il est accusé de vol de données confidentielles au bénéfice d'un partenaire commercial.
Petit rappel historique, Michael Leeper a démarré sa carrière chez Columbia en 2000, comme responsable de l'équipe en charge des PC. Il obtient des promotions pour atteindre le poste de directeur des infrastructures technologiques où il est en charge de la maintenance du système d'information de Columbia et de signer les contrats avec les fournisseurs technologiques. Il était en contact notamment avec Denali, un fournisseur qu'il a rejoint en 2014.

Rester dans le réseau de manière masquée

Mais, juste avant de partir, le responsable IT se serait créé un compte réseau sous le nom « Jeff Maning », aussi appelé « jmanning ». Ce qui lui aurait permis d'accéder au réseau de Columbia, y compris via le VPN et le VDI de la société. Un accès utilisé plus de 700 fois par Michael Leeper pendant 2 ans, afin de voler des documents sensibles de Columbia (plan d'affaires, budget IT, etc) au profit de Denali selon l'accusation. Il aurait mis en place une seconde backdoor (« svcmon ») liée à un compte utilisé par les administrateurs systèmes pour surveiller l'activité réseau. Avant de partir, Michael Leeper s'y serait octroyé le privilège maximal.
Dans sa plainte, Columbia estime que Michael Leeper a eu accès à des e-mails sur des accords commerciaux dans lesquels Denali avait des intérêts financiers. Le prestataire s'est défendu dans un communiqué en indiquant qu'une telle affaire « *ne reflète nullement la politique de Denali et ses valeurs* ». La société précise coopérer à l'enquête et a donné congé à son CTO, Michael Leeper, afin, officiellement, qu'il puisse organiser sereinement sa défense…[lire la suite]

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 d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Réagissez à cet article

Source : *Quand un DSI laisse des backdoors pour pirater son ancien employeur*

Bordeaux : des drones pour mettre des amendes sur les routes

Bordeaux : des drones pour mettre des amendes sur les routes

Comment les drones vont changer nos vies Progressivement, les avions sans pilote se déploient dans de multiples secteurs d'activité, mais le marché, prometteur, peine encore à décoller, freiné par la législation.…[Lire la suite]

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 sur cette page.

Réagissez à cet article

250 millions de PC infectés par un nouveau malware

250 millions de PC infectés par un nouveau malware

Après Wannacry, c’est au tour de Fireball de menacer les ordinateurs. Ce malware chinois ne bloque pas les machines pour exiger de l’argent, mais il détourne les recherches effectuées sur le navigateur et récupère discrètement les données.

Les internautes n’ont pas fini de s’arracher les cheveux à cause des virus informatiques. Après Wannacry qui bloquait les ordinateurs pour demander des rançons, voici le malware Fireball. Ce logiciel asiatique qui infecte les ordinateurs a été détecté par les experts de **Check Point**.
Il prend discrètement le contrôle d’un PC pour détourner les recherches et récupérer les données. Il aurait déjà infecté plus de 250 millions de machines dans le monde. Les zones géographiques les plus touchées sont l’Inde, le Brésil et l’Amérique, mais l’Europe et la France ne sont pas épargnées.

Ce logiciel n’est pourtant pas le fruit d’un gang de hackers. C’est officiellement un adware -nom donné aux logiciels publicitaires- qui a été développé en toute légalité par **Rafotech**, une agence de marketing digitale chinoise qui a pignon sur rue. Et pour le répandre, l’entreprise l’a inséré discrètement dans des suites logicielles téléchargeables gratuitement, tels que « FVP Imageviewer », « Deal Wifi » ou « SoSo Desktop ». Mais il ne se contente pas de diffuser de la pub.

Check Point – Diffusion mondiale de Fireball
Une fois installé, Fireball change la page d’accueil du navigateur pour afficher un faux moteur de recherche (« Trotux ») qui redirige les recherches vers des moteurs que l’utilisateur n’aura pas forcément choisis. Il va également installer un système de traçage pour collecter des données de navigation, mais aussi, selon Check Point, les mots de passe ou les numéros de cartes bancaires.
Fireball pourrait également prendre le contrôle d’une machine pour installer et d’exécuter à distance des logiciels espions. Il crée aussi une porte dérobée pour espionner ses victimes. Les experts en sécurité conseillent aux victimes de le supprimer au plus vite. Si la page d’accueil de votre PC a été modifiée sans votre intervention, il y a de grande chance qu’il ait été contaminé.
[Source : BFM Business]

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 d’expertises, d’audits, de formations et de sensibilisation dans toute la France et à l’étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d’un Correspondant Informatique et Libertés (CIL) ou d’un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l’Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d’informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Réagissez à cet article

Source : *Après Wannacry, c’est au tour de Fireball de menacer les ordinateurs. Ce malware chinois ne bloque pas les machines*

pour exiger de l’argent, mais il détourne les recherches effectuées sur le navigateur et récupère discrètement les données.

La Cnil veut protéger de manière effective les données des élèves

	La Cnil veut protéger de manière effective les données des élèves

---

La Commission nationale de l'informatique et des libertés (Cnil) veut fixer un cadre de régulation face au développement des offres de services numériques dans l'éducation.

Un appel à garantir la protection des données scolaires

Avec l'utilisation croissante des services numériques à l'école, la Cnil sollicite une action du ministère de l'Éducation nationale. La **Commission nationale de l'informatique et des libertés** appelle en effet la place Grenelle à garantir *« de façon effective et contraignante »* la protection des données scolaires. Dans un communiqué reçu ce mercredi, elle estime qu'il est *« plus que jamais nécessaire »* de fixer un cadre de régulation pour une protection de manière effective des données personnelles des élèves et des enseignants. Elle a notamment cité le **développement des offres de services numériques dans l'éducation** par les Gafam. Cet acronyme désignant les plus grands fournisseurs du web regroupe Google, Apple, Facebook, Amazon, Microsoft.

L'importance du respect des droits des personnes

Déjà annoncée au printemps 2016, cette **charte de confiance** est encore en cours de finalisation. La **Cnil** insiste alors sur le respect des droits des personnes. Selon elle, cette charte devrait garantir *« la non-utilisation des données scolaires à des fins commerciales, l'hébergement de ces données en France ou en Europe »*, rapporte *Europe1*. *« L'obligation de prendre des mesures de sécurité conformes aux normes en vigueur »* est également sollicitée…[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 dessins
Notre sélection d'articles sur le RGPD (Règlement Européen sur la Protection des données Personnelles) et les DPO (Délégués à la Protection des Données)

Notre métier : Vous accompagner dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Réagissez à cet article

Source : *Education: la Cnil veut protéger de manière effective les données des élèves – LINFO.re – France, Société*

Victime de cyberattaque ? Une plateforme d’aide aux victimes existe : ACYMA

	Victime de cyberattaque ? Une plateforme d’aide aux victimes existe : ACYMA

Le gouvernement a lancé une plateforme Internet d'aide aux victimes de piratage et autres cyberattaques.
L'ordinateur familial ne répond plus, victime d'un virus. Pis, ses données ont été cryptées par un rançongiciel comme le désormais célèbre Wannacry. Pas de panique. Hier, le gouvernement a lancé le site www.cybermalveillance.gouv.fr afin de répondre en urgence aux victimes d'attaques informatiques de plus en plus dangereuses.
Cette plate-forme met en relation des victimes – particuliers comme entreprises – avec des prestataires dans leur zone de vie. De plus, le site regorge de vidéos et de fiches pratiques afin d'adopter les bons réflexes d'hygiène numérique. La région Hauts-de-France sera à partir d'aujourd'hui zone de test. L'initiative sera généralisée à toute la France en octobre…[lire la suite]

Denis JACOPINI : Nous sommes prestataire inscrit sur la plateforme ACYMA (www.cybermalveillance.gouv.fr) depuis les premiers jours et en relation avec l'ANSSI depuis fin 2016 pour apporter nos compétences et notre expérience à ce projet .
Notre grande connaissance du monde de la cybercriminalité et les nombreuses expertises judiciaires sur lesquelles nous intervenons vous garantissent non seulement l'usage des meilleurs outils en matière d'investigation numérique (forensic) et un respect minutieux des procédures de respect de l'intégrité de la preuve pour un usage judiciaire des données collectées.
Nous pouvons intervenir indépendamment ou en assistance d'un huissier et nos dossiers peuvent être utilisés en justice.
Contactez-nous

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 d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Réagissez à cet article

Source : *Une plateforme d'aide en cas de cyberattaque – Le Parisien*