Satori, le botnet qui transforme vos objets connectés en zombies

Satori, le botnet qui transforme vos objets connectés en zombies

Depuis le mois de décembre, les experts en cybersécurité regardent avec inquiétude grossir à toute vitesse un botnet baptisé Satori. Ce dernier s'ajuste en permanence aux contre-mesures, et a la particularité de se loger dans tout objet mal protégé et connecté à Internet.

Parmi les cibles favorites de Satori, les thermostats, les TV connectées, les systèmes d'infotainment dans les voitures, mais surtout les routeurs. Une fois massif, le botnet pourrait servir à des attaques en déni de service (DDoS)…[lire la suite]

LE NET EXPERT

• ACCOMPAGNEMENT RGPD (ÉTAT DES LIEUX ⇒ MISE EN CONFORMITÉ)

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

• FORMATIONS / SENSIBILISATION :

- **CYBERCRIMINALITÉ**
- **PROTECTION DES DONNÉES PERSONNELLES**
- AU **RGPD**
- À LA **FONCTION DE DPO**

• RECHERCHE DE PREUVES (outils Gendarmerie/Police)

- ORDINATEURS (**Photos / E-mails / Fichiers**)
- TÉLÉPHONES (récupération de **Photos / SMS**)
- SYSTÈMES NUMÉRIQUES

• EXPERTISES & **AUDITS** (certifié ISO 27005)

- TECHNIQUES | JUDICIAIRES | ADMINISTRATIVES
- **SÉCURITÉ** INFORMATIQUE
- SYSTÈMES DE **VOTES ÉLECTRONIQUES**

Besoin d'un Expert ? contactez-nous

Notre Expert, Denis JACOPINI, est assermenté, spécialisé en **Cybercriminalité**, **Recherche de preuves** et en **Protection des données personnelles**. Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), en Droit de l'Expertise Judiciaire et certifié en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005), Denis JACOPINI est aussi formateur inscrit auprès de la DDRTEFP (Numéro formateur n°93 84 03041 84).

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

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

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Source : *Satori, le botnet qui transforme vos objets connectés en zombies*

Failles dans les microprocesseurs Meltdown & Spectre

Failles dans les microprocesseurs Meltdown & Spectre

Ces derniers jours, il y a eu beaucoup de bruit dans la sphère de la sécurité informatique. Les mots Meltdown et Spectre ont fait la une de plusieurs journaux et sites d'information, qu'ils soient spécialisés ou généralistes. Cet article est une mise à plat de ma compréhension du sujet, une explication qui j'espère permettra à d'autres de mieux comprendre les mécanismes et la portée de ces attaques.

Les mécanismes en jeu

Ces deux attaques sont différentes de celles dont nous entendons parler majoritairement. Elles touchent le matériel, ou *hardware*, et non pas des applications.
Pour comprendre ces attaques, il est nécessaire de faire un petit récapitulatif sur le fonctionnement et l'optimisation d'un processeur.

Fonctionnement d'un processeur

Un processeur, ce n'est rien d'autre qu'une calculatrice. Au début, des calculs étaient envoyés à un processeur, celui-ci effectuait les calculs qu'on lui envoyait dans l'ordre, les uns après les autres, puis il retournait les résultats.
Lorsqu'un programme est exécuté, les données à traiter sont dans la mémoire vive (qu'on appelle aussi simplement *mémoire*), ou RAM. Pour traiter une instruction, les données nécessaires au traitement doivent être envoyées depuis la mémoire vive vers la mémoire interne du processeur pour qu'il les traite. Ensuite, le résultat est enregistré à nouveau en mémoire.
Si le temps de traitement des données par le processeur est environ le même que le temps de récupération des données en mémoire, tout ça se coordonne très bien.
En effet, pendant que le processeur traite une instruction, les données de la prochaîne instruction sont rapatriées, permettant d'avoir un flux tendu.
Avec le temps, le matériel a évolué, et les processeurs sont devenus très, très rapides. Tellement rapides qu'ils ont largement devancé les accès en mémoire.
Ainsi, aujourd'hui, le traitement d'une instruction se fait environ en 0.5 nano-seconde, tandis qu'un accès mémoire se fait en 20 nano-secondes.
Par conséquent, si jamais le processeur traitait les instructions linéairement, il passerait la plupart de son temps à attendre les données, au lieu de travailler.
C'est pourquoi les constructeurs se sont penchés sur le sujet afin d'optimiser le processus de traitement de leurs processeurs…[lire la suite]

LE NET EXPERT
• **ACCOMPAGNEMENT RGPD (ÉTAT DES LIEUX ⇒ MISE EN CONFORMITÉ)**
- **ANALYSE DE VOTRE ACTIVITÉ**
- **CARTOGRAPHIE DE VOS TRAITEMENTS DE DONNÉES**
- **IDENTIFICATION DES RISQUES**
- **ANALYSE DE RISQUE (PIA / DPIA)**
- **MISE EN CONFORMITÉ RGPD** de vos traitements
- **SUIVI** de l'évolution de vos traitements
• **FORMATIONS / SENSIBILISATION :**
- **CYBERCRIMINALITÉ**
- **PROTECTION DES DONNÉES PERSONNELLES**
- AU **RGPD**
- À LA **FONCTION DE DPO**
• **RECHERCHE DE PREUVES** (outils Gendarmerie/Police)
- ORDINATEURS (**Photos / E-mails / Fichiers**)
- TÉLÉPHONES (récupération de **Photos / SMS**)
- SYSTÈMES NUMÉRIQUES
• **EXPERTISES** & **AUDITS** (certifié ISO 27005)
- TECHNIQUES | JUDICIAIRES | ADMINISTRATIVES
- **SÉCURITÉ** INFORMATIQUE
- SYSTÈMES DE **VOTES ÉLECTRONIQUES**

Besoin d'un Expert ? contactez-nous

Notre Expert, Denis JACOPINI, est assermenté, spécialisé en **Cybercriminalité**, **Recherche de preuves** et en **Protection des données personnelles**. Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), en Droit de l'Expertise Judiciaire et certifié en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005), Denis JACOPINI est aussi formateur inscrit auprès de la DDRTEFP (Numéro formateur n°93 84 03041 84).

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

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

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Source : *Attaques Meltdown & Spectre – hackndo*

La Cnil inflige une amende de

100 000 euros à Darty

	La Cnil inflige une amende de 100 000 euros à Darty

Le groupe est sanctionné pour ne pas avoir suffisamment sécurisé les données des clients ayant eu recours au service après-vente en ligne.

En février 2017, la CNIL a été informée de l'existence d'un incident de sécurité concernant le traitement des demandes de service après-vente des clients de la société ETABLISSEMENTS DARTY ET FILS.
Lors d'un contrôle en ligne réalisé début mars 2017 les équipes de la CNIL ont pu constater qu'une défaillance de sécurité permettait d'accéder librement à l'ensemble des demandes et des données renseignées par les clients de la société, via un formulaire en ligne de demande de service après-vente. Plusieurs centaines de milliers de demandes ou réclamations contenant des données telles que les nom, prénom, adresse postale, adresse de messagerie électronique ou numéro de téléphone des clients étaient potentiellement accessibles.

Le contrôle sur place réalisé quinze jours plus tard a révélé que le formulaire de demande de service après-vente, à l'origine du défaut de sécurité, avait été développé par un prestataire commercialisant un logiciel de service après-vente « sur étagère ». Lors du contrôle, la société ETABLISSEMENTS DARTY ET FILS a indiqué avoir recours à un autre formulaire distinct et ne pas utiliser celui à l'origine de l'incident.

Les vérifications opérées par la CNIL ont pourtant permis de constater que les fonctionnalités du logiciel rendant accessible le formulaire développé par son prestataire n'avaient pas été désactivées. Elles ont également révélé que le prestataire n'avait pas mis en place de filtrage des adresses URLs, qui aurait permis d'empêcher à des tiers non autorisés d'accéder aux données des clients contenues dans l'outil de gestion des demandes de service après-vente *via* le formulaire défectueux.
Alors même qu'elle avait informé la société de cet incident de sécurité, la CNIL a constaté que les fiches des clients étaient toujours accessibles entre le premier et le second contrôle et que de nouvelles fiches avaient été créées dans ce laps de temps. Le soir même du second contrôle, la société l'informait des mesures prises pour remédier à cet incident.
La Présidente de la CNIL a désigné un rapporteur afin que soit engagée une procédure de sanction à l'encontre de la société ETABLISSEMENTS DARTY ET FILS.

La formation restreinte de la CNIL a prononcé une sanction d'un montant de 100.000 euros, estimant que la société avait manqué à son obligation de sécurité des données personnelles, en méconnaissance de l'article 34 de la loi Informatique et Libertés.

La formation restreinte a considéré que le simple fait que la société fasse appel à un prestataire sous-traitant ne la décharge pas de son obligation de préserver la sécurité des données traitées pour son compte, en sa qualité de responsable du traitement.

La société aurait dû s'assurer préalablement que les règles de paramétrage de l'outil mis en œuvre pour son compte ne permettaient pas à des tiers non autorisés d'accéder aux données des clients. Cette vérification préalable d'absence de vulnérabilité fait partie des tests élémentaires qui doivent être réalisés par une société en matière de sécurité des systèmes d'information.
Par ailleurs, en sa qualité de responsable de traitement, la société aurait dû procéder de façon régulière à la revue des formulaires permettant d'alimenter l'outil de gestion des demandes de service après-vente. A ce titre, la formation restreinte a considéré qu'une bonne pratique en matière de sécurité des systèmes informatiques consiste à désactiver les fonctionnalités ou modules d'un outil qui ne seraient pas utilisés ou pas nécessaires.
La formation restreinte a néanmoins tenu compte notamment de l'initiative du responsable de traitement de diligenter un audit de sécurité après cette atteinte à la sécurité des données ainsi que de sa bonne coopération avec les services de la CNIL.
Pour approfondir
> Délibération n°SAN-2018-001 du 8 janvier 2018 Délibération de la formation restreinte n° SAN-2018-001 du 08/01/2018 prononçant une sanction pécuniaire à l'encontre de la société ETABLISSEMENTS DARTY ET FILS Etat: VIGUEUR

Faille non réparée après un premier contrôle
La Commission révèle en avoir rapidement informé Darty. Pourtant « la Cnil a constaté que les fiches des clients étaient toujours accessibles entre le premier et le second contrôle et que de nouvelles fiches avaient été créées dans ce laps de temps ».
Cette faille provenait en fait d'un logiciel de service après-vente proposé par un sous-traitant. Mais la Cnil a considéré « que le simple fait que la société fasse appel à un prestataire sous-traitant ne la décharge pas de son l'obligation de préserver la sécurité des données traitées pour son compte, en sa qualité de responsable du traitement »…[lire la suite]

Besoin d'un **accompagnement pour vous mettre en conformité avec le RGPD ?** ?
Besoin d'une **formation pour apprendre à vous mettre en conformité avec le RGPD** ?
Contactez-nous

A Lire aussi :
Mise en conformité RGPD : Mode d'emploi
Formation RGPD : L'essentiel sur le règlement Européen pour la Protection des Données Personnelles
Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016
DIRECTIVE (UE) 2016/680 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016
Le RGPD, règlement européen de protection des données. Comment devenir DPO ?
Comprendre le Règlement Européen sur les données personnelles en 6 étapes
Notre sélection d'articles sur le RGPD (Règlement Européen sur la Protection des données Personnelles) et les DPO (Délégués à la Protection des Données)

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

Denis 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 DIRTEF 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 : *DARTY : sanction pécuniaire pour une atteinte à la sécurité des données clients*

En matière de sécurité informatique, la faille, c’est l’humain

	**En matière de sécurité informatique, la faille, c’est l’humain**

En matière de sécurité informatique, la mise à jour régulière d'un antivirus performant est indispensable. Mais, à en croire l'expert Benoît Grunemwald, rien ne saurait remplacer l'éducation du « maillon faible » : l'humain.

Baptisée Eset, en hommage à la déesse de la guérison de la mythologie égyptienne, la petite entreprise née en 1992 à Bratislava (Tchécoslovaquie) est aujourd'hui le quatrième acteur mondial du secteur de la sécurité informatique. Ses antivirus arrivent régulièrement en tête des tests de fiabilité et de sécurité. Toujours détenue par ses trois cofondateurs, elle a réalisé 460 millions de chiffre d'affaires en 2016… et bloque 300.000 attaques par heure ! Benoît Grunemwald, directeur des opérations Eset France, livre ses conseils pour sécuriser au maximum les données d'une entreprise.

Management : Concrètement, à quoi s'expose une entreprise qui néglige sa sécurité informatique ?

Benoît Grunemwald : A une perte de productivité liée à l'arrêt de son système, à une fuite de données, et à une atteinte à son « e-réputation » avec une dégradation de son site Web ou son détournement dans le but de répandre des malwares…[lire la suite]

LE NET EXPERT

• **ACCOMPAGNEMENT RGPD (ÉTAT DES LIEUX ⇒ MISE EN CONFORMITÉ)**

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

• **FORMATIONS / SENSIBILISATION** :

- **CYBERCRIMINALITÉ**
- **PROTECTION DES DONNÉES PERSONNELLES**
- AU **RGPD**
- À LA **FONCTION DE DPO**

• **RECHERCHE DE PREUVES** (outils Gendarmerie/Police)

- ORDINATEURS (**Photos / E-mails / Fichiers**)
- TÉLÉPHONES (récupération de **Photos / SMS**)
- SYSTÈMES NUMÉRIQUES

• **EXPERTISES** & **AUDITS** (certifié ISO 27005)

- TECHNIQUES | JUDICIAIRES | ADMINISTRATIVES
- **SÉCURITÉ** INFORMATIQUE
- SYSTÈMES DE **VOTES ÉLECTRONIQUES**

Besoin d'un Expert ? contactez-nous

Notre Expert, Denis JACOPINI, est assermenté, spécialisé en **Cybercriminalité**, **Recherche de preuves** et en **Protection des données personnelles**. Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), en Droit de l'Expertise Judiciaire et certifié en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005), Denis JACOPINI est aussi formateur inscrit auprès de la DDRTEFP (Numéro formateur n°93 84 03041 84).

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

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

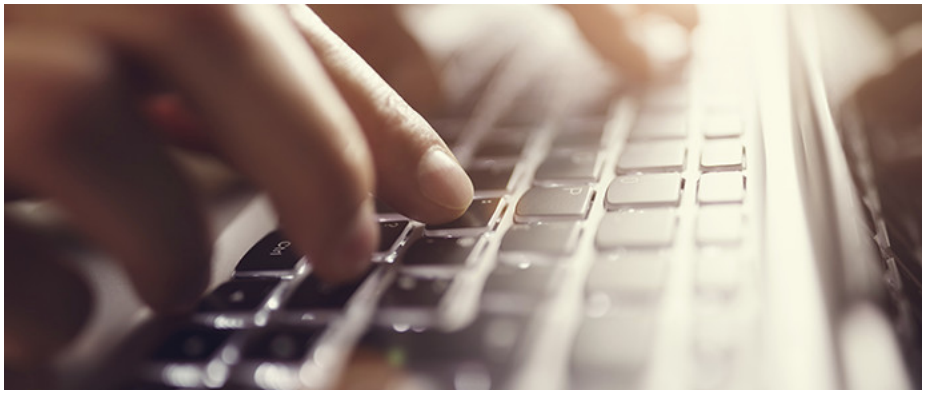
Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Source : *En matière de sécurité informatique, c'est l'humain qui est la faille – Capital.fr*

Alerte : Deux failles importantes découvertes. Mettez à jour !



Alerte : Deux failles importantes découvertes. Mettez à jour !

De quoi s'agit-il ? Le 3 janvier 2018, deux failles importantes de sécurité baptisées Meltdown et Spectre ont été révélées publiquement. Ces failles touchent à des niveaux variables les microprocesseurs de la très grande majorité des ordinateurs personnels (PC), mais aussi des serveurs informatiques, des tablettes, des téléphones mobiles (smartphones) dans le monde entier.

Quel est le risque ?

Un attaquant qui parviendrait à exploiter ces failles pourrait avoir accès aux informations personnelles des utilisateurs des machines vulnérables (données personnelles, mots de passe, coordonnées bancaires…).

Ces failles étaient connues depuis quelques mois maintenant des principaux constructeurs de microprocesseurs (Intel, AMD, ARM), des grands éditeurs de logiciels (Microsoft, Apple, Google, Mozilla…) ainsi que des éditeurs d'anti-virus qui préparaient depuis lors des correctifs de sécurité.

Suite aux révélations publiques de ces failles, la manœuvre s'accélère pour les corriger avant que les cybercriminels n'arrivent à en profiter et les premiers correctifs ont commencé à être diffusés.

Etes-vous concernés ?

Certainement. Comme évoqué ci-dessus, la grande majorité des ordinateurs, des tablettes, des téléphones mobile, mais aussi des serveurs dans le monde entier est touchée par ces failles. Ces failles concernent aussi bien les machines qui fonctionnent sous Microsoft Windows, que celles qui fonctionnent sous Apple macOS-iOS, Google Android ou les différentes versions de GNU/Linux.

Que devez-vous faire pour vous protéger ?

Vous assurer de bien installer toutes les mises à jour de sécurité que vous avez peut-être déjà reçues et que vous allez recevoir dans les prochains jours, semaines voire mois des éditeurs de vos systèmes d'exploitation (Microsoft, Apple, Google, GNU/Linux), de vos navigateurs Internet (Microsoft, Google, Mozilla, Apple…), de vos anti-virus.

Pensez à bien vérifier que tous les systèmes de vérification des mises à jour de vos équipements sont bien activés.

Pensez à contrôler également que les mises à jour de sécurité que vous réalisez proviennent bien de vos éditeurs et constructeurs. Des cybercriminels pourraient essayer de profiter de cet événement pour se faire passer pour vos éditeurs ou constructeurs et vous envoyer de fausses mises à jour qui contiendraient un virus. N'acceptez donc par exemple aucune mise à jour que vous recevriez par mail, car c'est une pratique totalement inhabituelle.

Si vous faites vos mises à jour, serez-vous complètement protégés ?

Ce n'est pas complètement certain. Rien ne permet même d'attester que ces failles pourront être intégralement corrigées. Mais les différents correctifs de sécurité qui seront diffusés rendront certainement la tâche bien plus difficile pour les cybercriminels qui voudraient en tirer partie.

Toutes ces mises à jour qui arrivent en même temps peuvent-ils produire des dysfonctionnements de vos matériels ?

Ce n'est pas impossible. Mais le risque de dysfonctionnement est certainement bien moindre que celui de se voir voler ses données personnelles les plus confidentielles (mots de passe, numéros de carte bancaire…) par des cybercriminels.

Vous avez entendu que vos matériels risquaient de ralentir après les mises à jour de sécurité, qu'en est-il ?

Ce n'est pas impossible non plus, mais il est bien trop tôt pour l'affirmer. Vous pouvez même ne pas constater la moindre différence. Quoiqu'il en soit, si tel était le cas, mieux vaut aller un peu moins vite en sécurité, que plus vite en prenant des risques inconsidérés.

Vous avez entendu que ces failles étaient difficilement exploitables, alors devez-vous vraiment en tenir compte ?

Oui, car la cybercriminalité ne cesse de progresser en compétence technique. La vague d'attaques par le rançongiciel (ransomware) Wannacry du printemps 2017 est là pour le rappeler. A peine quelques semaines après la révélation d'une vulnérabilité de haut niveau, les cybercriminels ont réussi à l'exploiter pour une attaque qui a frappé le monde entier.

En conclusion ?

Ces failles sont sérieuses et touchent tous les équipements informatiques ou presque. Il est donc primordial de se sentir concerné et d'appliquer avec sérieux toutes les mises à jour de sécurité officielles que vous recevez de vos constructeurs ou éditeurs

[Original sur cybermalveillance.gouv.fr]

LE NET EXPERT

• **ACCOMPAGNEMENT RGPD (ÉTAT DES LIEUX ⇒ MISE EN CONFORMITÉ)**

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

• **FORMATIONS / SENSIBILISATION :**

- **CYBERCRIMINALITÉ**
- **PROTECTION DES DONNÉES PERSONNELLES**
- AU **RGPD**
- À LA **FONCTION DE DPO**

• **RECHERCHE DE PREUVES** (outils Gendarmerie/Police)

- ORDINATEURS (**Photos / E-mails / Fichiers**)
- TÉLÉPHONES (récupération de **Photos / SMS**)
- SYSTÈMES NUMÉRIQUES

• **EXPERTISES** & **AUDITS** (certifié ISO 27005)

- TECHNIQUES | JUDICIAIRES | ADMINISTRATIVES
- **SÉCURITÉ** INFORMATIQUE
- SYSTÈMES DE **VOTES ÉLECTRONIQUES**

Besoin d'un Expert ? contactez-nous

Notre Expert, Denis JACOPINI, est assermenté, spécialisé en **Cybercriminalité**, **Recherche de preuves** et en **Protection des données personnelles**. Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), en Droit de l'Expertise Judiciaire et certifié en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005), Denis JACOPINI est aussi formateur inscrit auprès de la DDRTEFP (Numéro formateur n°93 84 03041 84).

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

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

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Source : *Alerte sécurité – Failles Meltdown & Spectre – CYBERMALVEILLANCE.GOUV.FR*

25% des cyberattaques cibleront les objets connectés en 2020

25% des cyberattaques cibleront les objets connectés en 2020

L'IoT présente des problématiques de sécurité particulièrement épineuses. La majorité des objets connectés ont fait l'impasse sur la sécurité, avec des options de configuration minimales, voire inexistantes sur le sujet, et une absence de protocoles d'authentification ou d'autorisation. La majorité des objets connectés ne dispose pas d'interface qui permet aux outils de sécurité de s'y installer, ce qui rend quasi-impossible le patching et les mises à jour. Dans ce contexte, il n'est guère étonnant que les experts s'attendent à ce que 25% des cyberattaques ciblent l'Internet des Objets en 2020.

L'expansion des réseaux IoT (objets connectés) instaure de nouvelles menaces pour la sécurité avec environ 22,5 milliards d'appareils connectés prévus d'ici 2021, selon un rapport de Business Insider. La sécurité représentera donc un défi de taille, mais les gros volumes de données engendrés par l'IoT pourraient en réalité aider les chercheurs à repérer les failles de sécurité. Encore faudrait il que les entreprises déclenchent enfin une cartographie rigoureuse de leur patrimoine informationnel. Selon une nouvelle étude de CyberArk, près de deux tiers des organisations françaises (62 %) ayant été victime d'une cyberattaque n'ont pas avoué à leurs clients que leurs données personnelles avaient été compromises. Avec l'entrée en vigueur du Règlement Général sur la Protection des Données (RGPD) en mai 2018, les entreprises qui n'agiront pas pour être plus transparentes s'exposeront à d'importantes sanctions.La mise en place du RGPD / GDPR en mai 2018 les incite « fortement »…[lire la suite]

LE NET EXPERT

• ACCOMPAGNEMENT RGPD (ÉTAT DES LIEUX ⇒ MISE EN CONFORMITÉ)

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

• FORMATIONS / SENSIBILISATION :

- **CYBERCRIMINALITÉ**
- **PROTECTION DES DONNÉES PERSONNELLES**
- AU **RGPD**
- À LA **FONCTION DE DPO**

• RECHERCHE DE PREUVES (outils Gendarmerie/Police)

- ORDINATEURS (**Photos / E-mails / Fichiers**)
- TÉLÉPHONES (récupération de **Photos / SMS**)
- SYSTÈMES NUMÉRIQUES

• EXPERTISES & **AUDITS** (certifié ISO 27005)

- TECHNIQUES | JUDICIAIRES | ADMINISTRATIVES
- **SÉCURITÉ** INFORMATIQUE
- SYSTÈMES DE **VOTES ÉLECTRONIQUES**

Besoin d'un Expert ? contactez-nous

Notre Expert, Denis JACOPINI, est assermenté, spécialisé en **Cybercriminalité**, **Recherche de preuves** et en **Protection des données personnelles**. Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), en Droit de l'Expertise Judiciaire et certifié en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005), Denis JACOPINI est aussi formateur inscrit auprès de la DDRTEFP (Numéro formateur n°93 84 03041 84).

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

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

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Source : *Cyberisques News – Cybersécurité : 25 Prévisions utiles pour 2018*

Les entreprises appelées à se prémunir contre la cybercriminalité

	**Les entreprises appelées à se prémunir contre la cybercriminalité**

Avec la démocratisation d'Internet, la cybercriminalité a évolué et prend désormais plusieurs formes. Les solutions de protection ne suffisent pas, une vraie stratégie de cybersécurité est nécessaire.

Les TPE-PME constituent aujourd'hui la cible de prédilection des cybercriminels. A la différence des grandes structures, ces entreprises ne disposent pas le plus souvent d'un DSI. Encore moins de process de formation et d'information leur permettant de prévenir efficacement les invasions virales et autres intrusions par voie numérique. Le phénomène est à portée internationale. En france, le baromètre du Club des experts de la sécurité de l'information et du numérique (CESIN) indique que 80% des entreprises interrogées ont été confrontées au problème au cours de 2016. Pourtant, seule une PME sur quatre a engagé une démarche de gestion des risques liés à la cybercriminalité d'après une étude de la même année menée par un assureur.

En savoir plus sur
http://lavieeco.com/news/la-vie-des-pme/les-entreprises-appelees-a-se-premunir-contre-la-cybercriminalite.html#CpIb5cqqvY5YWUrE.99…[lire la suite]

LE NET EXPERT

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

• **FORMATIONS / SENSIBILISATION** :
- **CYBERCRIMINALITÉ**
- **PROTECTION DES DONNÉES PERSONNELLES**
- AU **RGPD**
- À LA **FONCTION DE DPO**

• **RECHERCHE DE PREUVES** (outils Gendarmerie/Police)
- ORDINATEURS (**Photos / E-mails / Fichiers**)
- TÉLÉPHONES (récupération de **Photos / SMS**)
- SYSTÈMES NUMÉRIQUES

• **EXPERTISES** & **AUDITS** (certifié ISO 27005)
- TECHNIQUES | JUDICIAIRES | ADMINISTRATIVES
- **SÉCURITÉ** INFORMATIQUE
- SYSTÈMES DE **VOTES ÉLECTRONIQUES**

Besoin d'un Expert ? contactez-nous

Notre Expert, Denis JACOPINI, est assermenté, spécialisé en **Cybercriminalité, Recherche de preuves** et en **Protection des données personnelles**. Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), en Droit de l'Expertise Judiciaire et certifié en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005), Denis JACOPINI est aussi formateur inscrit auprès de la DDRTEFP (Numéro formateur n°93 84 03041 84).

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

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

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Source : *Les entreprises appelées à se prémunir contre la cybercriminalité – Lavieeco*

Un inquiétant malware cible les objets connectés de la planète

Un inquiétant malware cible les objets connectés de la planète

Un nouveau malware Botnet « Reaper » a été identifié par les spécialistes en cybersécurité. Ce logiciel malveillant cible particulièrement les appareils connectés et cherche à nuire à l'ensemble des réseaux de dispositifs IdO en usant de la technique du déni de se

Toute la planète est concernée par cette menace

Les experts de la cybersécurité estiment que ce malware a déjà attaqué environ 1 million d'appareils jusqu'à présent et poursuit sa propagation sans aucun problème. Du fait que ce logiciel malveillant n'a été repéré que récemment, il est encore difficile pour le moment de trouver la solution la plus efficace pour le détourner rapidement. De plus, les spécialistes qui l'ont découvert soulignent que l'objectif exact des hackers reste toujours inconnu. Ils se penchent encore sur les vraies intentions de ces malfaiteurs.

La solution pour se protéger de Reaper

La solution la plus pratique et la plus rapide proposée par les experts pour le moment est de changer les mots de passe de chaque dispositif reliés à Internet. Les appareils comme les caméras connectées ou les routeurs sans fil sont également exposés au risque d'infiltration. Ce procédé prend sans doute plus de temps. Néanmoins, les manuels fournis par la marque donnent généralement des instructions précises à ce sujet…[lire la suite]

LE NET EXPERT

• **FORMATIONS / SENSIBILISATION :**
- **CYBERCRIMINALITÉ**
- **PROTECTION DES DONNÉES PERSONNELLES**
- AU **RGPD**
- À LA **FONCTION DE DPO**

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

• **RECHERCHE DE PREUVES** (outils Gendarmerie/Police)
- ORDINATEURS (**Photos / E-mails / Fichiers**)
- TÉLÉPHONES (récupération de **Photos / SMS**)
- SYSTÈMES NUMÉRIQUES

• **EXPERTISES** & **AUDITS** (certifié ISO 27005)
- TECHNIQUES | JUDICIAIRES | ADMINISTRATIVES
- **SÉCURITÉ** INFORMATIQUE
- SYSTÈMES DE **VOTES ÉLECTRONIQUES**

Besoin d'un Expert ? contactez-nous

Notre Expert, Denis JACOPINI, est assermenté, spécialisé en **Cybercriminalité**, **Recherche de preuves** et en **Protection des données personnelles**. Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), en Droit de l'Expertise Judiciaire et certifié en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005), Denis JACOPINI est aussi formateur inscrit auprès de la DDRTEFP (Numéro formateur n°93 84 03041 84).

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Source : *« Reaper » : nouveau malware ciblant les objets connectés – @Sekurigi*

Formation RGPD : Ce n'est pas qu'une affaire de juristes

Formation RGPD ; Ce n'est pas qu'une affaire de juristes

Le 25 mai 2018, le règlement européen sera applicable. De nombreuses formalités auprès de la CNIL vont disparaître. En contrepartie, la responsabilité des organismes sera renforcée. Ils devront en effet assurer une protection optimale des données à chaque instant et être en mesure de la démontrer en documentant leur conformité.

Les 6 étapes recommandées par la CNIL pour vous préparer au RGPD sont :

1- DÉSIGNER UN PILOTE

Pour piloter la gouvernance des données personnelles de votre structure, vous aurez besoin d'un véritable chef d'orchestre qui exercera une mission d'information, de conseil et de contrôle en interne : le délégué à la protection des données. En attendant 2018, vous pouvez d'ores et déjà désigner un « correspondant informatique et libertés », qui vous donnera un temps d'avance et vous permettra d'organiser les actions à mener.

2- CARTOGRAPHIER VOS TRAITEMENTS DE DONNÉES PERSONNELLES

Pour mesurer concrètement l'impact du règlement européen sur la protection des données que vous traitez, commencez par recenser de façon précise vos traitements de données personnelles. L'élaboration d'un registre des traitements vous permet de faire le point.

3- PRIORISER LES ACTIONS À MENER

Sur la base de votre registre, identifiez les actions à mener pour vous conformer aux obligations actuelles et à venir. Priorisez ces actions au regard des risques que font peser vos traitements sur les droits et les libertés des personnes concernées.

4- GÉRER LES RISQUES

Si vous avez identifié des traitements de données personnelles susceptibles d'engendrer des risques élevés pour les droits et libertés des personnes concernées, vous devrez mener, pour chacun de ces traitements, une analyse d'impact sur la protection des données (PIA).

5- ORGANISER LES PROCESSUS INTERNES

Pour assurer un haut niveau de protection des données personnelles en permanence, mettez en place des procédures internes qui garantissent la prise en compte de la protection des données à tout moment, en prenant en compte l'ensemble des événements qui peuvent survenir au cours de la vie d'un traitement (ex : faille de sécurité, gestion des demande de rectification ou d'accès, modification des données collectées, changement de prestataire).

6- DOCUMENTER LA CONFORMITÉ

Pour prouver votre conformité au règlement, vous devez constituer et regrouper la documentation nécessaire. Les actions et documents réalisés à chaque étape doivent être réexaminés et actualisés régulièrement pour assurer une protection des données en continu.

Pour **cartographier vos traitements** de données personnelles, vous devrez avoir une méthode, des outils, collecter des informations à la fois techniques et organisationnelles.
Pour **prioriser les actions** à mener vous devrez identifier précisément les traitements à risques, les données sensibles et connaître les solutions techniques applicables.
Pour **gérer les risques**, vous devrez appliquer une méthode relative à cette obligation. Proche de la méthode EBIOS, l'analyse d'impact relative à la protection des données (DPIA) est le passage obligatoire pour tout organisme (entreprise ou association) disposant de salariés ou détenant des données sensibles appartenant à des tiers.
L'**organisation des processus internes** nécessite une excellente connaissance des menaces et des risques. Une certification relative à une norme ISO 27001 ou 27005 nous paraît essentielle.

Vous pouvez donc constater que pour chacun des points ci-dessus, le chef d'orchestre que doit être le DPO doit à la fois avoir une bonne connaissance du règlement Européen RGPD (ou GDPR en anglais) mais également connaître et maîtriser différents sujets tels que la sécurité informatique, différentes méthodes telles que l'analyse des flux de données et l'analyse de risques.

Ainsi, nous considérons qu'il serait inconscient d'aborder la mise en conformité avec le RGPD des établissements sans action conjointe d'un conseil juridique spécialisé en droit des données personnelles et d'une personne ayant une bonne connaissance de la sécurité informatique et de l'analyse de risques autour de des données.

Ceci n'est que mon avis, n'hésitez pas à me faire part du votre ou commenter ce post.

Besoin d'un **accompagnement pour vous mettre en conformité avec le RGPD ?** ?
Besoin d'une **formation pour apprendre à vous mettre en conformité avec le RGPD** ?
Contactez-nous

CONTENU DE NOTRE FORMATION RGPD :
Parce que les piratages sont de plus en plus fréquents et dangereux, à tout moment, nos données personnelles médicales, bancaires et confidentielles peuvent se retrouver dans la nature à cause d'un professionnel négligeant ayant manqué à son obligation de sécurité des données vis-à-vis de ses clients, salariés, fournisseurs…
Pour ne pas que vous deveniez ce professionnel négligeant risquant d'être sanctionné pénalement et par une mauvaise réputation, un règlement Européen (le RGPD) entrant en application le 25 mai 2018, clarifie les obligations que tous les professionnels devraient déjà respecter.
Venez découvrir lors de cette journée de formation les points importants de ce règlement Européen et la méthode à suivre pour continuer sereinement votre activité.

A Lire aussi :
Mise en conformité RGPD : Mode d'emploi
Formation RGPD : L'essentiel sur le règlement Européen pour la Protection des Données Personnelles
Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016
DIRECTIVE (UE) 2016/680 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016
Le RGPD, règlement européen de protection des données. Comment devenir DPO ?
Comprendre le Règlement Européen sur les données personnelles en 6 étapes
Notre sélection d'articles sur le RGPD (Règlement Européen sur la Protection des données Personnelles) et les DPO (Délégués à la Protection des Données)

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

---

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

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la 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 : Denis JACOPINI et *Règlement européen : se préparer en 6 étapes*

Alerte : Mettez à jour votre Mac s'il a la High Sierra, version 10.13

Alerte : Mettez à jour votre Mac s'il a la High Sierra, version 10.13

Une faille de sécurité préoccupante avait été détectée sur la dernière version, appelée « High Sierra », du système d'exploitation macOS d'Apple. La firme à la pomme a développé un correctif en urgence.

Comment savoir si vous êtes concerné ?

La vulnérabilité permettait d'obtenir un accès administrateur depuis un simple accès utilisateur, sans nécessairement nécessiter un accès physique à l'ordinateur : pour peu que des services à distance (comme par exemple VNC Viewer) soient activés, un intrus connecté à votre réseau local pouvait en prendre le contrôle. Il n'est toutefois pas possible de se *logger* par ce moyen sur une machine déjà allumée, dont l'écran est protégé par mot de passe. Apple avait rappelé la procédure permettant remédier temporairement au problème : il s'agit d'activer l'utilisateur « root » sur votre Mac et de définir un mot de passe.

VERSION.

Ce problème ne concerne que la dernière version du système d'exploitation (High Sierra, version 10.13). Pour savoir quelle est la version du système de votre Mac, il vous suffit de suivre le mode d'emploi mis en ligne par Apple : dans le menu Pomme situé dans le coin de l'écran, sélectionnez « *À propos de ce Mac* ». La version du système d'exploitation s'affiche dans la boîte de dialogue…[lire la suite]

Denis JACOPINI

Afin de connaître la version de Mac OS X installé sur votre ordinateur, veuillez suivre les manipulations suivantes :

1. Cliquez sur le menu Pomme en haut à gauche de votre écran.
2. Sélectionnez « A propos de ce Mac »
3. Une fenêtre va apparaître avec la version de votre système.

LE NET EXPERT

:

• **MISE EN CONFORMITÉ RGPD / CNIL**

- **AUDIT RGPD ET CARTOGRAPHIE** de vos traitements
- **MISE EN CONFORMITÉ RGPD** de vos traitements
- **SUIVI** de l'évolution de vos traitements

• **FORMATIONS / SENSIBILISATION :**

- **CYBERCRIMINALITÉ**
- **PROTECTION DES DONNÉES PERSONNELLES**
- AU **RGPD**
- À LA **FONCTION DE DPO**

• **RECHERCHE DE PREUVES** (outils Gendarmerie/Police)

- ORDINATEURS (**Photos / E-mails / Fichiers**)
- TÉLÉPHONES (récupération de **Photos / SMS**)
- SYSTÈMES NUMÉRIQUES

• **EXPERTISES** & **AUDITS** (certifié ISO 27005)

- TECHNIQUES | JUDICIAIRES | ADMINISTRATIVES
- **SÉCURITÉ** INFORMATIQUE
- SYSTÈMES DE **VOTES ÉLECTRONIQUES**

Besoin d'un Expert ? contactez-nous

Notre Expert, Denis JACOPINI, est assermenté, spécialisé en **Cybercriminalité**, **Recherche de preuves** et en **Protection des données personnelles**. Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), en Droit de l'Expertise Judiciaire et certifié en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005), Denis JACOPINI est aussi formateur inscrit auprès de la DDRTEFP (Numéro formateur n°93 84 03041 84).

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

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

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Source : *Une faille de sécurité critique détectée sur le système d'exploitation MacOS – Sciencesetavenir.fr*