Le réseau informatique des drones militaires américains piraté ?

	Le réseau informatique des drones militaires américains piraté ?

Le 9 septembre dernier, le réseau informatique de la base Creech de l'US Air Force, dans le Nevada, est tombé en panne, peut-être en raison d'un acte de piratage. C'est de là que sont conduites les opérations de surveillance et de bombardement par drones. Le réseau n'est toujours pas rétabli complètement.

L'armée américaine s'est-t-elle fait pirater le réseau de communication qu'elle utilise pour piloter à distance sa flotte de drones tueurs, qui bombardent quotidiennement dans de multiples pays du monde dont l'Afghanistan, la Syrie, le Pakistan, la Somalie, ou l'Irak ? La question se pose alors que BuzzFeed dévoile que l'US Air Force a reconnu que le réseau informatique de sa base Creech Air Force, dans le Nevada, était tombé en panne le 9 septembre dernier, et qu'il n'avait toujours pas pu être rétabli complètement depuis.
La base Creech Air Force est celle qui abrite les militaires qui, joystick à la main et yeux rivés sur un écran, déclenchent les frappes aériennes à des milliers de kilomètres de distance – parfois en utilisant uniquement des collectes de métadonnées pour présumer de l'identité des cibles, l'armée ayant développé des algorithmes pour les détecter. Les drones sont pilotés à travers des liaisons satellite qui permettent de relayer les ordres du Nevada jusqu'aux théâtres de guerre, avec un minimum de temps de latence et en toute sécurité.
Mais le système repose au moins partiellement sur le réseau SIRPnet (*Secret Internet Protocol Router Network*), une sorte de réseau Internet privé de l'armée américaine, utilisé pour véhiculer des informations confidentielles en toute sécurité. Or selon un appel d'offres étonnamment détaillé publié par l'armée, « *le système SIRPNet actuellement en opération à Creech AFB a échoué et des services essentiels ont été touchés* ». Elle précise que « *les systèmes ont été quelque peu restaurés avec l'utilisation de plusieurs appareils moins puissants* », et que « *cette solution temporaire a stabilisé les services, mais ne sera pas capable de satisfaire la demande encore très longtemps* ». Or, « *si cette solution échoue, il n'y actuellement aucun système de sauvegarde* »…[lire la suite]

Notre métier : Sensibiliser les décideurs et les utilisateurs aux risques liés à la **Cybercriminalité** et à la **Protection des Données Personnelles** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Denis JACOPINI anime dans toute le France et à l'étranger des conférences, des tables rondes et des formations pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles (Mise en Place d'un Correspondant Informatique et Libertés (CIL) dans votre établissement.
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

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

Contactez-nous

Réagissez à cet article

Original de l’article mis en page : Un système essentiel pour les drones tueurs américains est tombé en panne – Politique – Numerama

---

Plusieurs millions de clés de chiffrement plus du tout sécurisées

Plusieurs millions de clés de chiffrement plus du tout sécurisées

---

Des clés de chiffrement de 1024 bits utilisées pour sécuriser échanges Internet et VPN peuvent intégrer des « trappes » indétectables.

Des clés de chiffrement de 1024 bits utilisées pour sécuriser les échanges et les communications sur Internet (sites Web, VPN et serveurs), peuvent utiliser des nombres premiers munis de« *trappes* » indétectables. L'exploit permettrait à des pirates de déchiffrer plusieurs millions de communications chiffrées, et d'identifier les propriétaires des clés. C'est ce qui ressort des travaux d'une équipe de chercheurs : Joshua Fried et Nadia Heninger, de l'Université de Pennsylvanie, Emmanuel Thomé et Pierrick Gaudry, de l'équipe projet CARAMBA (Inria-CNRS-Université de Lorraine).

« *Nous démontrons dans nos travaux que la création et l'exploitation de trappes des nombres premiers (trapdoored primes) pour les standards d'échange de clés Diffie-Hellman et du DSA (Digital Signature Algorithm) est faisable pour les clés de 1024 bits avec des ressources informatiques universitaires modernes* », déclarent les chercheurs dans leur article technique. Ils disent avoir « *effectué un calcul de logarithmes discrets dans une trappe des nombres premiers, en deux mois sur un cluster académique* ».

Traffic HTTPS et VPN déchiffrés

Les standards internationaux de cryptographie reposent sur des nombres premiers dont l'origine devrait être vérifiable. Mais, aujourd'hui, trop de serveurs communiquent en s'appuyant sur des nombres premiers dont l'origine est invérifiable : 37% des sites en HTTPS (parmi le million de sites les plus visités du top Alexa) et 13% des VPN IPsec, rappelle Inria.

Pour son propriétaire, une clé de chiffrement dotée d'une trappe ressemble à toute autre clé fiable. Pour les attaquants qui exploiteraient la trappe, en revanche, la sécurité de la clé peut être brisée à travers la résolution plus rapide du problème du logarithme discret. Selon les chercheurs, l'échelle de difficulté pour un pirate deviendrait « *très facile* » pour une clé de 768 bits, « *facile* » pour une clé de 1024 bits, mais hors de portée pour du 2048 bits…. pour le moment…[lire la suite]

Notre métier : Sensibiliser les décideurs et les utilisateurs aux risques liés à la **Cybercriminalité** et à la **Protection des Données Personnelles** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).

Denis JACOPINI anime dans toute le France et à l'étranger des conférences, des tables rondes et des formations pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles (Mise en Place d'un Correspondant Informatique et Libertés (CIL) dans votre établissement.

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

---

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

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

Contactez-nous

Réagissez à cet article

Original de l’article mis en page : Des trappes dans plusieurs millions de clés de chiffrement

---

Spotify diffuserait des malwares

Spotify diffuserait des malwares

La version gratuite de Spotify diffuse en ce moment des publicités renvoyant vers des sites infestés de malwares. (CCM) – C’est quand on croit avoir tout vu qu’on était toujours le plus surpris.…[Lire la suite]

Denis JACOPINI anime des **conférences, des formations** en Cybercriminalité et est régulièrement invité à des **tables rondes en France et à l’étranger** pour sensibiliser les décideurs et les utilisateurs aux **Dangers liés à la Cybercriminalité (Arnaques, Piratages…) pour mieux s’en protéger** (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.

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

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

Contactez-nous

Réagissez à cet article

Une faille dans OpenSSH remet en question la sécurité de certains objets connectés

Une faille dans OpenSSH remet en question la sécurité de certains objets connectés

---

Akamai a découvert que les attaques DDoS IoT utilisées une faille dans OpenSSH existaient depuis 12 ans.

L'Internet des objets est en pleine croissance et la sécurité est au cœur des préoccupations des responsables informatiques. Qui plus est, ces objets connectés sont utilisés par des cybercriminels pour mener des attaques en déni de service. OVH et le spécialiste de la sécurité Brian Krebs en ont fait l'expérience ces dernières semaines.
On apprend maintenant que ces attaques ont été rendues possibles en raison d'une faille présente depuis 12 ans dans OpenSSH. Deux chercheurs d'Akamai, Ory Segal et Ezra Caltum ont découvert cette vulnérabilité et l'ont baptisé SSHowDowN Proxy. Elle vise notamment à enrôler plusieurs objets connectés comme les caméras de surveillance (CCTV) et leurs enregistreurs numériques (DVR), les antennes satellites, les routeurs, les NAS. « Ces dispositifs sont maillés pour attaquer une multitude de sites ou de services Internet à travers http, SMTP ou via un scan réseau », constate les experts. Ils ajoutent que les attaques peuvent aussi cibler les réseaux qui hébergent les objets connectés…[lire la suite]

Notre métier : Sensibiliser les décideurs et les utilisateurs aux risques liés à la **Cybercriminalité** et à la **Protection des Données Personnelles** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Denis JACOPINI anime dans toute le France et à l'étranger des conférences, des tables rondes et des formations pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles (Mise en Place d'un Correspondant Informatique et Libertés (CIL) dans votre établissement.
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

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

Contactez-nous

Réagissez à cet article

Original de l'article mis en page : Une faille dans OpenSSH âgée de 12 ans fragilise l'IoT

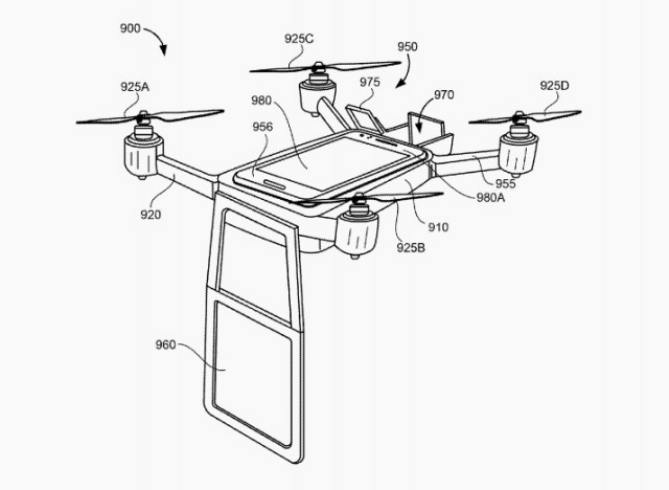
Google imagine un drone de télé-présence

Google imagine un drone de télé-présence

Il y a quelques mois, Google a obtenu un brevet concernant un concept de drone capable de servir de support pour de la télé-présence.

Google a un intérêt marqué pour les drones. En la matière, son projet le plus avancé s'appelle Wing et consiste à mettre au point un système de livraison de colis par les airs. Dévoilé en 2013, il doit faire ses débuts commerciaux l'année prochaine. D'ici là, grâce au feu vert de l'administration de l'aviation civile, Google va pouvoir effectuer des tests sur le territoire américain.

La firme de Mountain View a d'autres idées dans son sac. Il reste néanmoins à leur donner corps. C'est le cas par exemple de ce brevet repéré par Quartz qui décrit le principe d'un drone de type quadricoptère qui embarque plusieurs terminaux et équipements de façon à pouvoir afficher sur un écran l'image d'un interlocuteur situé à un autre endroit. En gros, c'est de la télé-présence déployée sur un drone.



On identifie sans peine l'écran et la tablette sur le drone…[lire la suite]

Notre métier : Sensibiliser les décideurs et les utilisateurs aux risques liés à la **Cybercriminalité** et à la **Protection des Données Personnelles** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).

Denis JACOPINI anime dans toute le France et à l'étranger des conférences, des tables rondes et des formations pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles (Mise en Place d'un Correspondant Informatique et Libertés (CIL) dans votre établissement.

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

---

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

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

Contactez-nous

Réagissez à cet article

Original de l'article mis en page : Google imagine un drone de télé-présence — Tech — Numerama

Drone piégé utilisé par l’EI contre deux militaires français

Drone piégé utilisé par l’EI contre deux militaires français

Selon des informations du Monde, deux militaires français qui étaient en opération auprès des Kurdes en Irak ont été rapatriés en France après avoir été grièvement blessé par un drone piégé de l'État islamique.

C'est un mode d'action que les forces de l'ordre redoutent sur le territoire national, et qui semble désormais déployé sur le terrain de l'adversaire. Le Monde affirme ce mardi que deux militaires français ont été gravement blessés par un drone qui avait été piégé par des militants de l'État islamique, en Irak. L'un des deux serait entre la vie et la mort.
« Les deux commandos ont été touchés par un drone volant piégé, envoyé par un groupe lié à l'EI, dans des circonstances qui restent à préciser. Les militaires auraient intercepté le drone, avant que celui-ci explose à terre. Ce mode d'action contre des forces françaises est en tout état de cause inédit », rapporte le quotidien, qui précise que ses informations sont confirmées par d'autres médias.
Ce piège aurait été tendu aux commandos parachutistes qui intervenaient auprès des forces kurdes à Erbil, dans le nord de l'Irak, entre Mossoul et Kirkouk. La ville est la capitale de la région autonome du Kurdistan.

Le Monde indique que le ministère de la Défense ne souhaite pas confirmer cette attaque d'un nouveau genre et le rapatriement des deux soldats à l'hôpital militaire de Percy-Clamart, non seulement par souci de protéger les familles, mais aussi peut-être en raison des « moyens employés pour cette attaque » (on peut ajouter que de manière plus générale s'agissant des propagandes de guerre, les armées n'aiment jamais communiquer sur leurs propres pertes, préférant mettre en avant leurs réussites pour conserver le moral des troupes et le soutien des populations).

LA CRAINTE D'UN ATTENTAT PAR DRONE
La crainte est sans doute que le mode opératoire, relativement peu coûteux et surtout peu risqué pour les attaquants, ne donne des idées sur le front irakien ou syrien, mais aussi en occident. L'hypothèse qu'une petite bombe puisse être transportée par un drone sans savoir d'où il a décollé et d'où il est contrôlé est soulevée depuis longtemps par les experts de la sécurité aérienne. Elle avait notamment été évoquée en France lors du survol des centrales nucléaires par des drones.
Depuis, le législateur s'est emparé du sujet en élaborant une proposition de régulation des drones en cours d'examen, qui prévoit notamment l'obligation d'identifier les drones à distance ou de brider leur utilisation dans certaines zones réglementées. Mais par définition les lois n'ont aucune influence contre ceux qui veulent les violer, et il paraît bien difficile d'empêcher totalement le transport de bombes par drone, sauf à utiliser des moyens technologiques encore balbutiants et impossibles à déployer sur tout le territoire comme des brouilleurs, des lasers, des perturbateurs de signaux GPS, des filets, ou même des aigles.

UNE RÉPONSE ARTISANALE À L'UTILISATION DE « ROBOTS TUEURS » ?
Le fait que les troupes de l'EI utilisent des bombes montées sur des drones n'est aussi, hélas, qu'une réponse attendue à l'utilisation croissante des drones et autres engins militaires conduits à distance par les troupes alliées. En août dernier, l'armée irakienne était fière de présenter un fusil mitrailleur monté sur un véhicule conduit à 1 km de distance, qui permettait d'aller tuer sans risquer de se faire tuer, ce qui est aussi l'objectif des avions de combat semi-autonomes, des navires de guerre ou des nouveaux chars d'assaut. L'utilisation de drones piégés n'est à cet égard qu'une réponse artisanale de même nature.
Il faut ajouter qu'en droit international, l'utilisation de telles armes n'est pas interdite dès lors qu'elles visent à tuer des militaires combattants, et non des civils. La question de la régulation des « robots tueurs » a déjà fait l'objet de débats dans la communauté internationale, dans le cadre de révisions des conventions de Genève, mais les perspectives d'un accord sont excessivement lointaines. La seule piste évoquée, encore très incertaine, est l'obligation qui pourrait être faite qu'un humain reste en permanence aux commandes des engins robotisés, pour ne pas parvenir à des guerres menées par IA interposées.
[Article source]

Original de l'article mis en page : L'État islamique aurait piégé un drone et blessé grièvement deux militaires français — Politique — Numerama

---

52 % des DSI Français acceptent moins de sécurité pour plus de mobilité

52 % des DSI Français acceptent moins de sécurité pour plus de mobilité

C'est une nouvelle à la fois peu surprenante et inquiétante : plus de la moitié des responsables informatiques en France cèdent du terrain sur le plan sécuritaire pour avantager la mobilité et le Bring Your Own Device.

« **Rendre les salariés et les opérations plus agiles** »
On ne cesse de le répéter depuis des années : le BYOD est loin d'être toujours un choix, il n'est pas rare qu'il s'impose de lui-même. Rejeter cette situation, c'est risquer une utilisation sous-marine, multipliant ainsi les risques. L'accepter, c'est limiter les risques en question en encadrant le BYOD.
Dans une étude menée par le cabinet Vanson Bourne pour le compte de VMware (plus de détails en fin d'article), nous apprenons que 52 % des responsables informatiques français font face à une telle pression vis-à-vis de la mobilité d'entreprise « qu'ils sont prêts à prendre des risques inconsidérés vis-à-vis de la sécurité des données de leur organisation ».
Ces risques sont en grande partie pris pour contenter les cadres dirigeants qui souhaitent absolument accéder aux données pro via leurs propres terminaux, « même si cela va à l'encontre des stratégies de leur entreprise » et que cela multiplie les risques de cyberattaques.
Mais les gains en valent la chandelle puisque les DSI cèdent. 51 % d'entre eux estiment ainsi que les bénéfices sont supérieurs aux risques. « Transformation numérique et mobilité sont indissociables. Les organisations doivent sans cesse chercher à développer leurs activités et à innover. Elles prennent donc des risques à court terme sur le plan de la sécurité afin de rendre les salariés et les opérations plus agiles » explique notamment Sylvain Cazard, directeur général de VMware France.
Pour s'adapter au marché et aux désirs de certains salariés, les DSI n'hésitent donc pas à prendre plus de risques. Il faut dire que près d'un quart des responsables informatiques estiment que le manque de mobilité des salariés réduit leur productivité. Un argument qui fait mouche et pousse logiquement les DSI à lâcher du lest côté sécurité.

Des salariés mal formés, des patrons sous-informés
Bien évidemment, les responsables n'ont pas à laisser la porte ouverte au premier pirate informatique venu. Une plus forte pédagogie auprès des salariés devient ainsi indispensable si l'entreprise ne souhaite pas voir toutes ses données partir dans la nature. Ce point est d'autant plus majeur sachant que l'étude indique que 60% des salariés mobiles précisent ne pas connaître la politique de sécurité de leur entreprise… Une statistique douloureuse et effrayante qu'il convient de ne pas minimiser.
Plus grave encore pour les dirigeants d'entreprises, une ancienne enquête de Vanson Bourne montrait que 25 % des DSI français ont confié ne pas informer leur patron en cas de cyberattaque. Ceci alors même que 29 % des DSI et 21 % des employés estiment que leurs patrons sont responsables en cas de fuite de données. Une incohérence qui en dit long sur la complexité de la problématique…[lire la suite]

Notre métier : Sensibiliser les décideurs et les utilisateurs aux risques liés à la **Cybercriminalité** et à la **Protection des Données Personnelles** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Denis JACOPINI anime dans toute le France et à l'étranger des conférences, des tables rondes et des formations pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles (Mise en Place d'un Correspondant Informatique et Libertés (CIL) dans votre établissement.
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

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

Contactez-nous

Réagissez à cet article

Original de l’article mis en page : BYOD : 52 % des DSI Français acceptent moins de sécurité pour plus de mobilité

Décryptage du réglement européen sur les données personnelles

	**Décryptage du réglement européen sur les données personnelles**

L'Association Française des Correspondants à la protection des Données Personnelles (AFCDP) a réalisé une version française commentée du règlement européen sur les données personnelles. Elle est disponible gratuitement en ligne

A compter du 25 mai 2018, le nouveau Règlement Européen 2019/679 sur la protection des données personnelles s'appliquera dans toutes les entreprises de l'Union Européenne. Ce texte modifie considérablement la législation en vigueur et fait peser des obligations nouvelles sur les responsables de traitements. L'AFCDP (Association française des correspondants à la protection des données personnelles) a réalisé une version française commentée de ce texte.
Le résultat de ce travail est librement accessible sur le site de l'association. Outre une rapide introduction et un index très complet, bien pratique pour retrouver des thèmes précis, l'essentiel du document est constitué par le texte même du Règlement. Les commentaires apparaissent dans une colonne sur le tiers de la page, en regard de la portion commentée. Si parfois, surtout au début, les commentaires se limitent à quelques mots, à d'autres moments ces commentaires explicitent en profondeur et contextualisent un article du Règlement.
Ne nous cachons pas que la simple mise en page du document en français est des plus agréables pour travailler. Les DSI et les directions juridiques ont en effet fort à faire d'ici 2018 et télécharger dès à présent ce document est donc des plus utiles.
Article original de Bertrand Lemaire

Réagissez à cet article

Le premier label Coffre-Fort Numérique a été délivré

Le premier label Coffre-Fort Numérique a été délivré

Un coffre-fort numérique est un espace de stockage numérique sécurisé, dont l'accès est limité à son seul utilisateur et aux personnes physiques qu'il a spécialement habilitées à cet effet.…[Lire la suite]

Denis JACOPINI anime des **conférences, des formations** sur la mise en conformité CNIL, des formations sur la protection des données Personnelles et est régulièrement invité à des **tables rondes en France et à l'étranger** pour sensibiliser les décideurs et les utilisateurs aux **obligations et moyens de se mettre en conformité avec le RGPD, futur règlement européen relatif à la Protection des Données Personnelles** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Plus d'informations sur notre page formations.

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

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

Contactez-nous

Réagissez à cet article

Pourquoi les vols de données sont en forte hausse ?

Pourquoi les vols de données sont en forte hausse ?

Une étude du Ponemon Institute pour Varonis révèle que la plupart des collaborateurs disposent d'accès trop importants, ce qui multiplie les dommages lorsque leurs comptes sont compromis

Trois entreprises sur quatre ont été victimes de la perte ou du vol de données importantes au cours des deux dernières années. Selon une nouvelle enquête menée auprès de plus de 3 000 collaborateurs et informaticiens aux États-Unis et en Europe, cela représente une très forte augmentation depuis 2014. Le rapport publié aujourd'hui a été rédigé par le Ponemon Institute et sponsorisé par Varonis Systems, Inc., principal fournisseur de solutions logicielles permettant de protéger les données contre les menaces internes et les cyberattaques.
Selon l'enquête, l'augmentation de la perte et du vol des données est en grande partie due aux compromissions de comptes internes. Celles-ci sont aggravées par des accès aux informations critiques bien plus permissifs que nécessaire par les collaborateurs et les tiers. Sans oublier le constant défaut de supervision des accès et de l'activité dans les systèmes de messagerie et les systèmes de fichiers, là où se trouvent les données les plus sensibles et les plus confidentielles.
Parmi les principales conclusions :
• 76 % des informaticiens indiquent que leur entreprise a fait l'expérience de la perte ou du vol de ses données au cours des deux dernières années. Ce chiffre représente une augmentation importante par rapport aux 67 % d'informaticiens interrogés ayant donné la même réponse lors de l'étude de 2014 réalisée par Ponemon pour le compte de Varonis.
• Les informaticiens indiquent que la négligence des collaborateurs a deux fois plus de chances d'entraîner la compromission des comptes internes que tout autre facteur, y compris les attaquants externes ainsi que les collaborateurs ou les prestataires malveillants.
• 78 % des informaticiens déclarent être très préoccupés par les ransomware, un type de logiciels malveillants qui bloque l'accès aux fichiers jusqu'au paiement d'une somme d'argent. 15 % des entreprises ont déjà fait l'expérience des ransomware et seule une petite moitié d'entre elles a détecté l'attaque au cours des 24 premières heures.
• 88 % des utilisateurs finaux indiquent que leur travail exige l'accès et l'emploi d'informations propriétaires telles que des données relatives aux clients, des listes de contacts, des renseignements sur les collaborateurs, des rapports financiers, des documents commerciaux confidentiels ou d'autres actifs informationnels critiques. C'est nettement plus que les 76 % enregistrés dans l'étude de 2014.
• **62 % des utilisateurs finaux indiquent avoir accès à des données de l'entreprise qu'ils ne devraient probablement pas pouvoir consulter**.
• Seuls 29 % des informaticiens interrogés indiquent que leur entreprise applique un modèle strict de moindre privilège pour s'assurer que les collaborateurs ont accès aux données de l'entreprise en fonction de leur besoin de les connaître.
• Seulement 25 % des entreprises supervisent toute l'activité relative à la messagerie et aux fichiers, alors que 38 % ne supervisent aucune activité.
• 35 % des entreprises ne disposent d'aucun enregistrement interrogeable de l'activité du système de fichiers, ce qui les rend incapables de déterminer les fichiers chiffrés par ransomware (entre autres choses).
Le rapport d'étude intitulé « *Closing Security Gaps to Protect Corporate Data: A Study of U.S. and European Organizations* » se fonde sur des entretiens menés en avril et mai 2016 auprès de 3 027 employés aux États-Unis, au Royaume-Uni, en France et en Allemagne. L'ensemble des personnes interrogées comprend 1 371 utilisateurs finaux ainsi que 1 656 informaticiens et professionnels de la sécurité informatique issus d'entreprises de tailles variant de quelques douzaines à plusieurs dizaines de milliers d'employés. Ils proviennent de divers secteurs, dont les services financiers, le secteur public, le secteur des soins de santé et des sciences de la vie, la vente au détail, le secteur industriel, le secteur technologique et l'industrie du logiciel…[lire la suite]

Denis Jacopini anime des **conférences et des formations** et est régulièrement invité à des **tables rondes en France et à l'étranger** pour sensibiliser les décideurs et les utilisateurs aux **CyberRisques** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Nous animons **conférences et formations** pour sensibiliser décideurs et utilisateurs **aux risques en informatique**, découvrir et comprendre les **arnaques** et les **piratages informatiques** pour mieux s'en protéger et se **mettre en conformité avec la CNIL** en matière de **Protection des Données Personnelles**. Nos actions peuvent être personnalisées et organisées dans votre établissement.
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

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

Contactez-nous

Réagissez à cet article

Original de l'article mis en page : Vols de données en forte hausse, cause principale: les menaces internes | Docaufutur