L’usurpation d’identité sur le web confirmée en Cassation

Dans un arrêt du 16 novembre 2016 repéré par Legalis, la Cour de cassation a rejeté le pourvoi formé par un ingénieur informaticien contre l’arrêt de la cour d’appel de Paris.…[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.

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 nouvelle doctrine en matière de cybersécurité

Une nouvelle doctrine en matière de cybersécurité

Jean-Yves Le Drian, ministre de la Défense, a inauguré hier un nouveau bâtiment de 9 000 m2 au centre DGA maîtrise de l'information à Bruz, près de Rennes. À cette occasion, il a dévoilé les grandes lignes de la nouvelle doctrine cyber des armées françaises. Elle reposera sur trois piliers : le renseignement, la protection/défense et la lutte informatique offensive.

« **L'irruption du numérique dans toutes les activités de la vie quotidienne nous oblige à repenser en profondeur l'art de la guerre.** » Hier, à Bruz, au sud de Rennes, dans les locaux de DGA maîtrise de l'information, « **le cœur battant du ministère de la Défense** », Jean-Yves Le Drian a présenté les grandes lignes de la nouvelle doctrine cyber des armées françaises.

Des combattants numériques

Cette doctrine s'appuiera sur trois piliers, a expliqué le ministre de la Défense. D'abord le renseignement, « **pour détecter les actions hostiles et leurs auteurs.** ». Ensuite, la protection et la défense : « **Nous devons bâtir d'épaisses murailles numériques.** » Enfin, la lutte informatique offensive : « **Nous avons besoin de combattants numériques pour riposter et neutraliser les cyber agresseurs.** »

Jean-Yves Le Drian a annoncé la création, en janvier 2017, d'un commandement français des opérations cyber (le « **CyberCom** »), placé sous la responsabilité directe du chef d'état-major des armées.

Ministre de la Cyberdéfense

C'est donc un Jean-Yves Le Drian, « **ministre de la Cyberdéfense** »,qui a passé la journée de lundi en Bretagne. Il a commencé par inaugurer officiellement le Pôle d'excellence cyber à Rennes. Cette association regroupe les chercheurs, les écoles et universités, les entreprises, les collectivités et les industriels qui œuvrent dans le numérique, la cybersécurité et la cyberdéfense.

Deuxième inauguration, un peu plus tard, dans les locaux de la DGA (direction générale de l'armement), à Bruz, au sud de Rennes. C'est ici que sont mis au point tous les systèmes d'information et de communication et les équipements électroniques des forces armées.

Le bâtiment baptisé Louis Pouzin – du nom d'un ingénieur français, précurseur d'Internet – est un bâtiment « **de haute qualité cyber** » qui accueille 270 experts sur 9 000 m2. Il est équipé de plus de 7 000 capteurs de sécurité, de 4 000 prises de réseau, dont 2 000 en fibre optique, le tout enveloppé dans 7 000 m3 de béton. Ici, des ingénieurs travaillent, entre autres, à détecter et à mettre hors d'état de nuire, les ennemis qui veulent capter les conversations téléphoniques des personnalités françaises, ou qui entendent prendra la main, à distance, sur la conduite des véhicules…[lire la suite]

Réagissez à cet article

Original de l'article mis en page : Le Drian annonce une nouvelle doctrine en matière de cybersécurité

L’essentiel Online – La surveillance au travail pourrait être modifiée – Luxembourg

	La surveillance au travail pourrait être modifiée

Les députés se sont penchés lundi sur le nouveau cadre concernant la protection des données au Grand-Duché.

Un patron pourrait bientôt ne plus avoir besoin de demander une autorisation préalable à la Commission nationale pour la protection des données (CNPD) avant de placer ses employés sous vidéosurveillance au travail. Cette mesure fait partie d'un projet de loi concernant la protection des données privées que les députés ont commencé à étudier lundi et qui s'inscrit dans le nouveau règlement européen qui entrera en vigueur le 25 mai 2018.

Le texte supprime la liste de traitement des données qui est aujourd'hui soumis à autorisation préalable de la CNPD, dont les traitements effectués à fin de surveillance. La CNPD fera, selon le projet de loi, des contrôles a posteriori, dans un but de simplification administrative. Un changement qui a suscité l'inquiétude de plusieurs députés, soucieux de protéger les citoyens d'une surveillance illégale par leurs employeurs.

La Chambre des salariés avait émis un avis défavorable en novembre, «dénonçant d'emblée la suppression de l'autorisation préalable (…). Elle s'oppose plus particulièrement, et de manière formelle, à cette exemption en faveur des traitements à des fins de surveillance sur le lieu de travail», expliquant que la loi actuelle, de 2002, «traduisait justement la volonté expresse du législateur luxembourgeois de protéger les personnes physiques de certains traitements « susceptibles de présenter des risques particuliers au regard des droits et libertés des personnes concernées »». À noter que le projet de loi introduit également des sanctions financières.
(JW/JV/*L'essentiel*)

Réagissez à cet article

Original de l’article mis en page : L’essentiel Online – La surveillance au travail pourrait être modifiée – Luxembourg

---

Cybercriminalité en région : une victime raconte son « traumatisme »

Cybercriminalité en région : une victime raconte son « traumatisme »

La lutte contre la cybercriminalité se joue aussi en région. Parmi les victimes de ces nouvelles pratiques de fraude numérique, des particuliers mais aussi des entreprises. Bruno a récemment vécu une attaque informatique dans son agence immobilière à Lunel. Il raconte.

C'était il y a un mois, au retour d'un week-end. Bruno rouvre son agence immobilière et se retrouve sans téléphone. La société qui gère son système de téléphonie déportée le prévient alors : « Nous vous avons coupé parce que nous nous sommes rendu compte qu'il y avait un problème. » Les lignes de l'entreprise ont en fait été victimes durant le week-end d'un hacker. Lequel a pu se brancher sur ses lignes et les a dirigées vers un service surtaxé au lieu du bas prix initial choisi par le chef d'entreprise et son opérateur.

« Et s'ils avaient pris nos fichiers ? »

Repérée très rapidement, la fraude n'aura eu que peu d'incidence financière : « 300 à 400 euros de téléphone volé, précise Bruno. Mais c'est un véritable traumatisme ! Quand j'ai appris ça, il y a eu dix minutes de flottement, où je me suis posé beaucoup de questions ! Ce n'est pas tant ce qu'ils m'ont volé, mais ce qu'ils auraient pu faire. Ils ont pu rentrer. Et s'ils avaient pris nos fichiers ? Quasiment toutes nos données sont informatisées… Ils peuvent foutre en l'air une entreprise ! » Cinq cents dossiers de propriétaires et leur historique, toute la comptabilité de l'agence…

Bruno a immédiatement porté plainte à la gendarmerie de Lunel. « Ils ont un super-service. Ils ont été à l'écoute, ont pris le problème au sérieux et très rapidement, ils sont remontés jusqu'à la source, dans un pays lointain. Vers Israël, je crois. Ils ont retrouvé le hacker, même s'il est impossible d'aller le chercher. Vous vous rendez compte de ce que ces gens sont capables de faire ! » Et de saluer le travail d'investigations des militaires.

« Les gens paient. Ils n'ont pas d'autre choix. »

Ces derniers rencontrent d'ailleurs souvent ce type de piratage des autocom ces derniers temps, avec des montants qui peuvent s'envoler à plusieurs dizaines de milliers d'euros si la fraude n'est pas détectée assez tôt. Bruno, lui, a finalement été remboursé par son opérateur. Il a renforcé son système de façon simple.

Ce qui n'empêche pas l'inquiétude de se retrouver un jour avec ses données prises en otage ou chiffrées… « J'ai plusieurs collègues qui ont répondu à des e-mails et qui se sont retrouvés victimes d'un chantage. Les gens paient. Ils n'ont pas d'autre choix » explique-t-il…[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 : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

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

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

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

Original de l’article mis en page : Cybercriminalité en région : une victime raconte son « traumatisme »

Prévisions cybercriminalité pour 2017

	**Prévisions cybercriminalité pour 2017**

Nous sommes tombés sur cet article sur le site Internet « Informaticien.be » et n'avons pas pu nous empêcher de le partager avec vous tant il est en accord avec les prévisions ressorties de nos analyses. Aux portes de 2017, les entreprises, administrations et association non seulement vont devoir s'adapter à une réglementation Européenne risquant s'impacter lourdement la réputation des établissements qui devront signaler à la CNIL qu'elle viennent d'être victime de piratage, mais également, l'évolution des techniques de piratage vont augmenter les risques qu'auront les organismes à se faire pirater leurs systèmes informatiques. N'hésitez pas à consulter notre page consacrée aux bons conseils que nous prodiguons depuis de nombreuses années sur https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles.
Denis JACOPINI

Trend Micro présente son rapport annuel des prévisions en matière de sécurité: 'The Next Tier – 8 Security Predictions for 2017'. L'année prochaine sera marquée par des attaques de plus grande envergure à tous les niveaux. Les cybercriminels adopteront des tactiques différentes pour tirer parti de l'évolution du paysage technologique.
« Nous pensons que la General Data Protection Regulation (GDPR) va non seulement changer fondamentalement la manière dont les entreprises gèrent leurs données, mais aussi induire de nouvelles méthodes d'attaque. La tactique du ransomware va également s'étendre pour toucher plus d'appareils, tandis que la cyberpropagande influencera de plus en plus l'opinion publique", déclare Raimund Genes, CTO de Trend Micro.
En 2016, l'on a assisté à une formidable augmentation des vulnérabilités d'Apple avec pas moins de 50 fuites. A cela s'ajoutent 135 bugs Adobe et 76 bugs Microsoft. Alors que Microsoft continue d'améliorer ses facteurs limitatifs et qu'Apple est de plus en plus considéré comme le système d'exploitation prépondérant, ce déplacement apparent des 'exploits' des logiciels vulnérables va encore s'accentuer en 2017.
L'IoT et l'IIoT – dans la ligne de mire des attaques ciblées
L'Internet of Things (IoT – internet des objets) et l'Industrial Internet of Things (IioT – internet industriel des objets) seront de plus en plus dans la ligne de mire des attaques ciblées en 2017. Ces attaques tirent parti de l'engouement croissant suscité par les appareils connectés en exploitant les failles et les systèmes non protégés et en perturbant des processus d'entreprise. L'usage croissant d'appareils mobiles pour surveiller les systèmes de production dans les usines et les milieux industriels, combiné au nombre important de vulnérabilités dans ces systèmes constitue une réelle menace pour les organisations.
Explosion de l'extorsion professionnelle
Le Business E-mail Compromise (BEC) et le Business Process Compromise (BPC) représentent de plus en plus une forme relativement simple et économiquement rentable d'extorsion professionnelle. En incitant un employé innocent à verser de l'argent sur le compte bancaire d'un criminel, une attaque BEC peut rapporter 140.000 dollars. Bien que le piratage direct d'un système de transaction financière exige plus d'efforts, cela représente une manne de pas moins de 81 millions de dollars pouvant tomber aux mains des criminels.
Autres faits marquants du rapport
Le nombre de nouvelles familles de ransomware ne progresse que de 25 %. Mais le ransomware s'étend désormais aux appareils IoT et aux terminaux informatiques autres que les desktops (par exemple les systèmes POS ou les distributeurs automatiques).
Les fournisseurs ne parviendront pas à protéger à temps les appareils IoT et IIoT pour éviter des attaques DoS (refus de service) ou d'autres types d'attaques.
Le nombre de failles découvertes dans les technologies Apple et Adobe augmente, ce qui vient s'ajouter aux « exploit-kits ».
46 pour cent de la population mondiale est aujourd'hui reliée à l'internet : la cyberpropagande ne va cesser d'augmenter, à présent que les nouveaux dirigeants des grands pays sont en place. L'opinion publique risque donc d'être influencée par de fausses informations.
Comme ce fut le cas lors de l'attaque de la Banque du Bangladesh plus tôt cette année, les cybercriminels parviennent à modifier des processus d'entreprise via des attaques BPC, et à en tirer largement profit. Les attaques BEC restent d'actualité pour extorquer des fonds à des employés qui ne se doutent de rien.
Le GDPR produira des changements de politique et administratifs qui auront un lourd impact sur les coûts. Cela exigera aussi des examens complexes des processus de données pour assurer la conformité réglementaire.
De nouvelles méthodes d'attaques ciblées déjoueront les techniques de détection modernes, permettant aux criminels de s'attaquer à différentes organisations.
Original de l'article mis en page : Le ransomware s'étend aux appareils connectés et à l'internet des objets – Press Releases – Informaticien.be

---

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

---

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

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

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

Original de l’article mis en page : Le ransomware s’étend aux appareils connectés et à l’internet des objets – Press Releases – Informaticien.be

---

Votre caméra IP peut-elle être piratée ?

Votre caméra IP peut-elle être piratée ?

Deux équipes de chercheurs ont découvert des failles de sécurité qui affectent des dizaines de modèles de caméras IP professionnelles et grand public.
Le malware Mirai n'a pas fini de lever des armées d'objets connectés corrompus pour lancer des attaques DDoS. Des chercheurs autrichiens de SEC Consult ont découvert que pas moins de 80 modèles de caméras IP Sony étaient accompagnées de backdoor d'origine exploitable par des pirates.

Les modèles IPELA Engine de Sony affectés

Les experts de SEC Consult ont précisément découvert deux comptes utilisateurs, et leurs mots de passe, non documentés, pour accéder aux caméras IPELA Engine du constructeur japonais. Des systèmes de vidéo surveillance principalement utilisés par les entreprises et les autorités. Ces comptes, baptisés « primana » et « debug » installés par défaut, pourraient être utilisés par des pirates pour prendre le contrôle du serveur Web intégré dans le périphérique depuis Internet (via Telnet/SSH, les services de commandes à distance des objets connectés) en plus d'un accès depuis le réseau local.
Ces « portes dérobées » sont généralement introduites par les développeurs du constructeur à des fins de maintenance ou de test à distance. Ou parfois par des organisations étatiques (comme dans le cas de la backdoor de la NSA sur des routeurs Juniper). Un accès distant qui se transforme en faille de sécurité quand il tombe entre de mauvaises mains (ce qui fut le cas pour Juniper, notamment).

Le correctif de Sony à appliquer en urgence

Pour SEC Consult, il ne fait aucun doute que ces accès backdoor *« permettent à un attaquant d'exécuter du code arbitraire sur les caméras IP concernées [et les] utiliser pour pénétrer le réseau et lancer d'autres attaques, perturber la fonctionnalité de l'appareil, envoyer des images manipulées, ajouter des caméras dans un botnet type Mirai ou espionner les gens »*. La référence à Mirai n'est pas neutre. Le malware s'était emparé de centaine de milliers d'objets connectés, essentiellement des caméras IP, pour lancer des attaques contre le fournisseur de services DNS Dyn, des clients d'OVH ou encore le site du journaliste spécialisé en sécurité Brian Krebs.
Sony a fourni une mise à jour du firmware. A installer avant que des individus malveillants ne se chargent de reconfigurer l'accès des caméras. Selon l'outil en ligne Censys.io, plus de 4 500 de ces caméras Sony vulnérables sont accessibles directement depuis Internet. Dont 1 510 aux Etats-Unis et 256 en France.

Des centaines de milliers de caméras résidentielles

Sony est loin d'être le seul acteur concerné par la sécurité de ses caméras IP. En parallèle, des chercheurs de la firme israélienne Cybereason déclarent avoir découvert au moins deux failles zero day dans une douzaine de familles de caméras IP vendues en marque blanche dans la grande distribution et notamment sur eBay ou Amazon. D'une part, ils ont identifié que le mot de passe du compte par défaut était le même pour tous les modèles de périphérique (« 888888 » en l'occurrence pour l'identifiant « admin »). Mot de passe qu'il est impossible de renforcer puisque le système refuse la combinaison de différents types de caractères (soit uniquement des chiffres, soit des caractères en minuscule ou en majuscule). Une fois identifié, l'utilisateur peut injecter des commandes dans la caméra à partir d'un serveur Web.
D'autre part, les experts ont trouvé un moyen d'accéder à l'objet même si celui-ci est protégé derrière un firewall, en passant par le serveur web du vendeur qui offre un service Cloud (pour visualiser les images à distance sur un PC ou smartphone). Les chercheurs ne détaillent pas la façon dont ils ont procédé. Mais, sur leur blog, ils assurent que *« cet exploit affecte des centaines de milliers de caméras dans le monde entier et nous ne voulons pas que les personnes malintentionnés utilisent nos recherches pour attaquer des gens ou utiliser ces caméras dans de futures attaques botnet »*…[lire la suite]

Original de l'article mis en page : Backdoor et Zero Days pour plusieurs milliers de caméras IP

Ce que les entreprises doivent savoir pour se mettre en conformité avec Règlement européen de protection des données en vigueur dans 18

mois

	Ce que les entreprises doivent savoir pour se mettre en conformité avec Règlement européen de protection des données en vigueur dans 18 mois

Entré en vigueur en mai 2016, le RGPD (Règlement général sur la protection des données) modifie les règles de gestion des données à caractère personnel dans les entreprises. Fin mai 2018, toutes les organisations devront être en conformité. Il vous reste donc moins de 18 mois pour mener ce chantier.

Qui est concerné?

Le RGPD s'applique « au traitement de données à caractère personnel, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier. » Ce règlement s'applique à toute structure (responsable de traitement des données ou sous-traitant) ayant un établissement dans l'Union européenne ou bien proposant une offre de biens ou de services visant les personnes qui se trouvent sur le territoire de l'Union européenne. Les actions de profilage visant cette cible sont également concernées. Ainsi, alors que la loi Informatique et libertés se basait sur des critères d'établissement et de moyens de traitement, le règlement européen 16-679 introduit la notion de ciblage: le critère principal d'application est désormais le traitement des données d'une personne se trouvant au sein de l'UE.

Qu'est-ce qu'une donnée à caractère personnel?

L'une des difficultés posées par le RGPD va consister à définir les données personnelles concernées. Le règlement stipule qu'il s'agit de « toute information concernant une personne physique identifiée ou identifiable », directement ou indirectement. Des données indirectement identifiantes, telles qu'un numéro de téléphone, ou un identifiant, sont donc concernées. De même, les données comportementales collectées sur Internet (notamment recueillies dans le cadre d'actions marketing de profilage), si elles sont corrélées à une identité, deviennent des données à caractère personnel. Selon le traitement appliqué aux données, des informations non identifiantes peuvent ainsi devenir identifiantes, par croisement des informations collectées. À noter, le RGPD prévoit des exceptions selon les traitements concernés, notamment au niveau des traitements de données RH (recrutement, contrat de travail…), pour lesquels les États membres peuvent prévoir « des règles plus spécifiques pour assurer la protection des droits et libertés » (article 88).

Quelles obligations pour les entreprises?

La loi Informatique et libertés se basait sur du déclaratif initial et des contrôles ponctuels. Le nouveau règlement européen remplace cette obligation de déclaration par une obligation de prouver à chaque moment que l'entreprise protège les données. Dès lors, la structuration même des outils permettant la collecte des données (CRM, DMP, solutions de tracking ou de géolocalisation…), mais aussi les contrats passés avec les sous-traitants et clients sont impactés. « Le règlement couple des notions techniques et juridiques », souligne Thomas Beaugrand, avocat au sein du cabinet Staub & Associés. Il introduit des nouveaux principes et concepts qui renvoient désormais vers plus de précautions techniques. Par ailleurs, les entreprises ont, entre autres, l'obligation de donner la finalité précise de la collecte des données (il s'agit du principe de minimisation, un des grands principes de la dataprotection, qui impose que seules les données nécessaires à la finalité poursuivie pourront être collectées).

Le GRPD impose également le principe de conservation limitée des données, ainsi que celui de coresponsabilité des sous-traitants et des entreprises en matière de protection de la data, qui permet de distribuer les responsabilité en fonction de la mainmise de chacun sur les données.

Enfin, parmi les changements majeurs, la nomination d'un DPO, ou délégué à la protection des données, qui sera obligatoire dans tout le secteur public, ainsi que dans les structures privées qui font des traitements de données exigeant un suivi régulier et systématique des personnes à grande échelle (dans le secteur du marketing, notamment). Il sera le garant de la conformité au règlement (voir encadré en page suivante)…[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 : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

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

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

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

Original de l’article mis en page : Règlement européen de protection des données: les nouvelles règles de gestion des données

---

Tracfin : le renseignement financier cible la FinTech

Tracfin : le renseignement financier cible la FinTech

Financement participatif détourné, paiement mobile opaque, transactions virtuelles anonymes… Tracfin met l'accent sur les risques numériques et appelle la FinTech à coopérer. Son objectif : mieux lutter contre le blanchiment de capitaux et le financement du terrorisme.

Tracfin, la cellule française de renseignement financier, a remis ce jeudi au ministre de l'Économie et des Finances, Michel Sapin, son rapport d'analyse des risques de blanchiment de capitaux et de financement du terrorisme. Financement participatif détourné, paiement mobile opaque, transactions virtuelles anonymes… Tracfin met l'accent sur les risques numériques émergents.

Selon le rapport, *« les risques d'escroquerie dans la finance participative (crowdfunding) sont élevés, par exemple par le détournement des paiements ou par l'élaboration de fraudes du type pyramide de Ponzi »*, surtout pour les plateformes de prêt. Quant aux plateformes de dons et de cagnottes en ligne, elles sont exposées à des risques *« importants de blanchiment de capitaux et de financement du terrorisme »*,. Certes, les fonds collectés restent limités, mais ils ont tout de même été multipliés par deux entre 2014 et 2015, observe Tracfin. **196,3 millions d'euros** ont été collectés via les plateformes de prêt l'an dernier, 50,3 millions d'euros pour l'investissement et 50,2 millions d'euros pour les dons.

Cadre européen pour le financement participatif

En France, un cadre juridique dédié au financement participatif a été mis en place en 2014. Il impose aux plateformes de prêt et d'investissement le choix d'un statut de conseiller en investissement participatif (CIP), régulé par l'Autorité des marchés financiers (AMF), ou d'intermédiaire en financement participatif (IFP), régulé par l'Autorité de contrôle prudentiel et de résolution (ACPR). Ces plateformes sont donc bien assujetties au dispositif national de lutte contre le blanchiment de capitaux et le financement du terrorisme (**LCB/FT**).

En revanche, la démarche restait facultative pour les plateformes de dons et les cagnottes en ligne. Mais elles seront aussi soumises à ce régime à partir de 2017, une ordonnance transposant une directive européenne dans ce domaine ayant été publiée le 2 décembre. C'est une bonne chose pour le directeur de Tracfin, Bruno Dalles, qui recommande l'adoption d'un cadre règlementaire dédié au financement participatif à l'échelle européenne. Car le cadre réglementaire national ne s'applique pas aux plateformes qui proposent, depuis l'étranger, d'effectuer des dons, prêts ou investissements…[lire la suite]

Réagissez à cet article

Original de l’article mis en page : Tracfin : le renseignement financier cible la FinTech

---

Norman Girard, Varonis : 3 statistiques qui montrent que les malwares sont encore là pour un moment

En juin dernier la police russe arrêtait 50 pirates suspectés d’attaques par malware contre des banques. C’est l’une des plus importantes arrestations de hackers de l’histoire de la Russie et les cybercriminels présumés ont volé plus de 45 millions de dollars aux banques attaquées.…[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.

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 entreprise touchée toutes les 40 secondes par une attaque par Ransomware en 2016

Une entreprise touchée toutes les 40 secondes par une attaque par Ransomware en 2016

Entre janvier et septembre 2016, la fréquence des attaques de ransomware contre les entreprises a triplé, passant d'une toutes les deux minutes une toutes les 40 secondes. Pour les particuliers, cet intervalle s'est réduit de 20 à 10 secondes. Avec l'apparition de plus de 62 nouvelles familles de logiciels rançonneurs au cours de l'année, le ransomware est la menace désignée comme fait marquant de l'année 2016. La rubrique Story of the Year fait partie de l'édition annuelle du Kaspersky Security Bulletin retraçant les principales menaces et statistiques de l'année écoulée et établit des prévisions sur ce que nous réserve 2017.

Le ransomware est devenu un réel business

Entre autres choses, 2016 a révélé à quel point le modèle RaaS (Ransomware as a Service) séduit désormais les criminels qui ne possèdent pas les compétences ou les ressources nécessaires pour développer leur propre malware ou n'en ont tout simplement pas envie. Le principe consiste pour les créateurs du code malveillant à offrir celui-ci « à la demande », en se bornant à vendre des versions modifiées à leurs clients qui les diffusent via du spam ou des sites web et reversent une commission à l'auteur, le principal bénéficiaire financier. « Le modèle classique de l'affiliation paraît aussi efficace pour le ransomware que pour les autres types de malware. Les victimes paient souvent la rançon, de sorte que l'argent coule à flots. Inévitablement, cela a conduit à l'apparition quasi quotidienne de nouveaux logiciels de cryptage », commente Fedor Sinitsyn, analyste senior en malware chez Kaspersky Lab.

L'évolution du ransomware en 2016

En 2016, le ransomware a poursuivi ses ravages à travers le monde, devenant de plus en plus élaboré et diversifié pour renforcer son emprise sur les données, les appareils, les particuliers et les entreprises :

• Les attaques sur les entreprises ont nettement augmenté. Selon l'étude Kaspersky Lab, une entreprise sur cinq au niveau mondial a subi un incident de sécurité informatique à la suite d'une attaque de ransomware et une petite entreprise sur cinq n'a jamais récupéré ses fichiers, même après avoir versé une rançon.

• Si certains secteurs d'activité ont été plus durement touchés que d'autres, notre étude indique que personne n'est véritablement épargné par le risque : le plus fort taux d'attaques frappe l'enseignement (de l'ordre de 23 %) et le plus faible, la grande distribution et les loisirs (16 %).

• Le ransomware « éducatif », conçu pour donner aux administrateurs système un outil permettant de simuler des attaques de ce type, a été rapidement et impitoyablement exploité par des criminels, donnant notamment naissance à Ded_Cryptor et Fantom.

• Parmi les méthodes de rançonnage observées pour la première fois en 2016 figure le cryptage de disque, consistant pour les auteurs des attaques à bloquer l'accès, non pas à quelques fichiers, mais à la totalité d'entre eux simultanément. Petya Dcryptor, alias Mamba, va encore plus loin en verrouillant l'ensemble du disque dur, grâce à des attaques de mots de passe par force brute pour accéder à distance aux appareils des victimes.

• Le ransomware Shade a montré sa capacité à changer d'approche vis-à-vis d'une victime si l'ordinateur infecté s'avère appartenir à des services financiers, pour télécharger et installer un spyware au lieu de crypter les fichiers.

• Les codes malveillants ont sensiblement perdu de leur qualité : c'est ainsi que de simples chevaux de Troie rançonneurs, présentant des erreurs de programmation et des fautes grossières dans les demandes de rançon, multiplient les risques pour les victimes de ne jamais récupérer leurs données…[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 : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

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

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

Le Net Expert INFORMATIQUE Cybersécurité & Conformité Contactez-nous

Réagissez à cet article

Original de l'article mis en page : Ransomware : Kaspersky Lab recense une attaque toutes les 40 secondes contre les entreprises en 2016 — Global Security Mag Online