

Les entreprises françaises toujours trop exposées aux risques de cyber-attaque

Denis JACOPINI



vous informe

Les entreprises
françaises
toujours
trop exposées
aux risques de
cyber-attaque



Tendances actuelles et émergentes pour la cybersécurité en 2017





Original de l'article mis en page : Sophos : tendances actuelles et émergentes pour la cybersécurité en 2017 – Global Security Mag Online

CryptXXX : ne payez pas la rançon !



Le match entre les instigateurs du ransomware CryptXXX et les chercheurs en sécurité se poursuit de plus belle. Kaspersky Lab a mis au point un outil de déchiffrement gratuit qui permet de débloquent les fichiers pris en otages par la troisième version de ce nuisible...[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.



[Contactez-nous](#)

Réagissez à cet article

CryptXXX : ne payez pas la

rançon !



CryptXXX : ne payez pas la rançon !

Le match entre les instigateurs du ransomware CryptXXX et les chercheurs en sécurité se poursuit de plus belle. Kaspersky Lab a mis au point un outil de déchiffrement gratuit qui permet de débloquent les fichiers pris en otages par la troisième version de ce nuisible...[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.



[Contactez-nous](#)

Réagissez à cet article

Pourquoi les DSI sont-ils inquiets à l'approche des Fêtes de fin d'année ?

	<p>Pourquoi les DSI sont-ils inquiets à l'approche des Fêtes de fin d'année ?</p>
---	---

La dernière étude d'IFS sur les défis auxquels les DSI sont confrontés durant la période des fêtes de fin d'années révèle que 76% des sondés se sentent davantage préoccupés à l'approche de cette période et ce, pour plusieurs raisons : la disponibilité du personnel (41% des répondants), les risques de piratage liés à la sécurité IT (31%) ainsi que les besoins IT des collaborateurs travaillant à distance (31% également). Tout cela a un impact certain sur les processus et activités métier.

De tous, les plus inquiets quant à la disponibilité du personnel à la période des fêtes de fin d'année sont les français. 62% d'entre eux déclarent qu'il s'agit de l'une de leurs plus grandes préoccupations au cours de la saison des fêtes de fin d'année. À l'opposé, près de la moitié des répondants américains (48%) citent le piratage informatique.

Du côté des « besoins », 42% des décideurs IT sont en demande d'un budget plus important. La migration vers le Cloud (18%) et le recrutement de personnel IT (16%) sont également cités dans le top 3 de leurs besoins. Par ailleurs, un quart des répondants américains et suédois (respectivement 26% et 25%) souhaitent, à court terme, une accélération de la migration vers le Cloud, alors qu'ils ne sont que 11% et 14% en Australie et Allemagne à privilégier cet enjeu.

« Ce qui ressort clairement de notre étude est que de nombreux décideurs IT ont des craintes légitimes pour la période des fêtes de fin d'année : disponibilité du personnel, risque de piratage informatique, commente Mark Boulton, CMO d'IFS. Il est essentiel que toutes les entreprises, quelle que soit leur taille, se préparent à affronter les problèmes qui pourraient survenir et soient en mesure d'accompagner, à distance, leurs collaborateurs ». L'IoT et la migration vers le Cloud faisant partie des solutions possibles.

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.



[Contactez-nous](#)



Réagissez à cet article

Original de l'article mis en page : Pourquoi les DSI sont-ils inquiets à l'approche des Fêtes de fin d'année ?

Rakos, un nouveau botnet qui vise aussi les objets connectés

<p>Denis JACOPINI</p>  <p>vous informe</p>	<p>Rakos, un nouveau botnet qui vise aussi les objets connectés</p>
--	---

Après Mirai, voici venir Rakos, un malware infectant des serveurs et des réseaux d'objets connectés, tournant sous Linux, afin de créer des botnets. ET, demain, lancer des attaques DDoS.

Comme le tristement célèbre malware Mirai, Rakos prend pour cible l'Internet des objets (IoT). Ces deux logiciels malveillants compromettent en effet des serveurs sous Linux et des réseaux d'appareils connectés. La capacité de nuisance de ces botnets contrôlés à distance est bien réelle. Si Mirai se propage essentiellement via les ports logiciels Telnet, Rakos vise lui les ports SSH. Les périphériques embarqués et les serveurs ayant un port SSH ouvert ou un mot de passe très faible sont les plus exposés. Rakos a été découvert cet été par les chercheurs de ESET.

À ce jour, Rakos est utilisé pour mener des attaques par force brute, indique l'entreprise dans un billet de blog. Et ce, afin d'ajouter d'autres appareils compromis à son réseau de machines zombies. Mais le programme pourrait également servir à mener des campagnes de spam ou des attaques par déni de service distribué (DDoS) d'ampleur, comme l'a fait Mirai...[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.



[Contactez-nous](#)

Réagissez à cet article

Original de l'article mis en page : Rakos, un nouveau botnet IoT en constitution

En 2017, les pirates informatiques vont mettre les bouchées doubles



En 2017, les pirates informatiques vont mettre les bouchées doubles

Les hackers vont notamment chercher à ébranler la confiance que l'on porte aux données, annonce un rapport de CyberArkBy SHOSHANNA SOLOMON

Les cyber-criminels du monde entier devraient intensifier leur activité l'année prochaine en utilisant l'intelligence artificielle et la manipulation des sources d'information pour créer des attaques plus fortes et plus dévastatrices, mettent en garde les experts de CyberArk.

En infiltrant et en manipulant les sources d'information, les pirates s'efforceront de saper la confiance des gens dans l'intégrité des données qu'ils reçoivent, utiliseront l'intelligence artificielle pour mener des cyber-attaques plus sophistiquées et augmenteront la collaboration entre eux pour déclencher un plus grand désordre, selon les prévisions cybersécuritaires pour 2017.

« L'intégrité de l'information sera l'un des plus grands défis auxquels les consommateurs, les entreprises et les gouvernements du monde devront faire face en 2017, où les informations venant de sources vénérées ne seront plus dignes de confiance », ont déclaré les experts.

« Les cyber-attaques ne se concentreront pas seulement sur une entreprise spécifique, il y aura des attaques contre la société visant à éliminer la confiance elle-même ».

Les attaquants ne se contentent pas d'accéder à l'information : ils « contrôlent les moyens de changer l'information là où elle réside et la manipulent pour les aider à atteindre leurs objectifs », affirment les auteurs.

Un Cyber-chercheur de CyberArk Kobi Ben-Naim (Crédit : Autorisation)

Un Cyber-chercheur de CyberArk Kobi Ben-Naim (Crédit : Autorisation)

Manipuler l'information – dans une campagne électorale par exemple – peut être un outil puissant. L'altération de contenus inédits, comme les fichiers audio, pourrait conduire à une augmentation des tentatives d'extorsion, en utilisant des informations qui peuvent ne pas être réelles ou prises hors de leur contexte.

« Il sera plus facile que jamais de rassembler des informations réelles volées dans une brèche avec des informations fabriquées, pour créer un déséquilibre ce qui rendra plus difficile pour les gens de déterminer ce qui est réel et ce qui ne l'est pas ».

L'augmentation de l'utilisation mobile, du web et des médias sociaux sont parmi les facteurs clés contribuant à l'augmentation explosive des cyber-menaces, a déclaré MarketsandMarkets, une firme de recherche basée au Texas, dans un rapport. La semaine dernière, Yahoo a subi le plus grand piratage au monde connu à ce jour, dans lequel la société a découvert une violation de sécurité vieille de 3 ans qui a permis à un pirate de compromettre plus d'un milliard de comptes d'utilisateurs.

Le marché mondial de la cyber-sécurité atteindra plus de 170 milliards de dollars d'ici 2020, selon une estimation de MarketsandMarkets, avec des entreprises qui se concentrent globalement sur les solutions de sécurité mais aussi sur les services...[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 téléphoniques, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DCTEP n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



[Contactez-nous](#)

Réagissez à cet article

Original de l'article mis en page : Les pirates informatiques vont mettre les bouchées doubles en 2017 | The Times of Israël

Une cyberattaque crée une nouvelle coupure électrique en Ukraine ?



Une cyberattaque
crée une
nouvelle coupure
électrique en
Ukraine ?

Suite à une nouvelle panne de courant, la compagnie nationale d'électricité de l'Ukraine enquête pour savoir si une attaque de cyberpirates est à l'origine du problème.

Des experts en sécurité cherchent à savoir si la panne de courant qui a affecté ce week-end certains quartiers de la capitale ukrainienne, Kiev, et la région environnante provient d'une cyberattaque. Si ce dernier point venait à être confirmé, il s'agirait du deuxième black-out causé par des pirates informatiques en Ukraine, après celle qui s'est produite en décembre 2015.

✖ L'incident a affecté les systèmes de commande d'automatisation d'un relais de puissance près de Novi Petrivtsi, un village situé au nord de Kiev, entre samedi minuit et dimanche. Cela a entraîné une perte de puissance complète pour la partie nord de Kiev sur la rive droite du Dniepr et la région environnante...

75 minutes pour rétablir le courant

Les ingénieurs d'Ukrenergo, la compagnie d'électricité ukrainienne, ont commuté l'équipement de commande en mode manuel et commencé à rétablir la puissance par palier de 30 minutes, a dit Vsevolod Kovalchuk, directeur d'Ukrenergo, dans un billet posté sur Facebook. Il a fallu 75 minutes pour restaurer toute la puissance électrique dans les zones touchées de la région, où les températures descendent jusqu'à -9 en ce moment. Une des causes suspectées est « une interférence externe à travers le réseau de données » a déclaré sans plus de précision Vsevolod Kovalchuk. Les experts en cybersécurité de la société étudient la question et publieront très bientôt un rapport.

Parmi les causes possibles de l'accident figurent le piratage et un équipement défectueux, a déclaré Ukrenergo dans un communiqué. Les autorités ukrainiennes ont été alertées et mènent une enquête approfondie. En attendant, les premières conclusions, tous les systèmes de commande ont été basculés du mode automatique au manuel, a indiqué la compagnie.

Un Etat derrière les attaques sophistiquées

Si un piratage venait à être confirmé, ce serait la seconde cyberattaque en un an contre le réseau électrique ukrainien. En décembre dernier, juste avant Noël, des pirates informatiques avaient lancé une attaque coordonnée contre trois compagnies d'électricité régionales ukrainiennes. Ils avaient réussi à couper l'alimentation de plusieurs sous-stations, provoquant des pannes d'électricité qui ont duré entre trois et six heures et touché les résidents de plusieurs régions.

A l'époque, les services de sécurité ukrainiens, le SBU, avaient attribué l'attaque à la Russie. Bien qu'il n'y ait aucune preuve définitive liant ces attaques au gouvernement russe, les cyberattaquants avaient utilisé un morceau de malware d'origine russe appelé BlackEnergy, et la complexité de l'attaque suggère l'implication d'un État. La semaine dernière, des chercheurs du fournisseur de sécurité ESET ont alerté la communauté au sujet d'attaques récentes contre le secteur financier ukrainien menées par un groupe qui partage de nombreuses similitudes avec le groupe BlackEnergy...[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.



[Contactez-nous](#)

Réagissez à cet article

5 à 10% du budget d'une entreprise devrait être consacrée à la cybersécurité



La sécurité a un cout mais ce n'est pas grand-chose comparé au prix à payer lorsqu'on est victime d'une attaque informatique.

Toutes les entreprises sont des cibles potentielles mais les secteurs des nouvelles technologies, des systèmes d'information, des médias, du transport et de logistique, de la grande distribution sont exposés à des pertes financières lourdes.

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.



[Contactez-nous](#)

Réagissez à cet article

Original de l'article mis en page : Les 5 chiffres à connaître de la cybersécurité – BeRecruited

Les particuliers victime d'une attaque par Ransomwares toutes les 10 secondes



Les particuliers
victime d'une
attaque par
Ransomwares
toutes les 10
secondes

Entre janvier et septembre 2016, le nombre d'attaques de ransomware contre les entreprises a triplé. En septembre, Kaspersky Lab enregistrait une attaque de ce type toutes les 40 secondes contre une toutes les 2 minutes en début d'année. Une entreprise sur cinq dans le monde est concernée.

Selon un rapport de l'entreprise de sécurité Kaspersky Lab, entre janvier et septembre 2016, la fréquence des attaques de ransomware contre les entreprises est passée de deux minutes à 40 secondes. Pour le grand public, la situation est encore pire : en septembre, la fréquence des attaques est passée à 10 secondes. Au cours du troisième trimestre de l'année, Kaspersky Lab a détecté 32 091 nouvelles versions de ransomware contre seulement 2 900 au cours du premier trimestre. « Au total, nous avons comptabilisé 62 nouvelles familles de malwares de cette catégorie cette année », a indiqué l'entreprise de sécurité. Ce nombre montre aussi très clairement l'intérêt des cybercriminels pour ce type de malwares dont la réussite reste constante malgré les actions menées par les autorités policières et judiciaires et les outils de décryptage gratuits fournis par les chercheurs et les entreprises de sécurité.

✖ L'enquête réalisée par Kaspersky Lab montre aussi que les petites et moyennes entreprises ont été les plus touchées : au cours des 12 derniers mois, 42 % d'entre elles ont été victimes d'une attaque par un ransomware. Parmi elles, une PME sur trois a payé la rançon, mais une sur cinq n'a jamais récupéré ses fichiers après le paiement. « Au total, 67 % des entreprises touchées par un ransomware ont perdu une partie ou la totalité de leurs données d'entreprise et une victime sur quatre a passé plusieurs semaines à essayer de retrouver l'accès à ses fichiers », ont déclaré les chercheurs de Kaspersky. Cette année, le ransomware le plus populaire est indéniablement CTB-Locker, utilisé dans 25 % des attaques. Viennent ensuite Locky, pour 7 % des attaques, et TeslaCrypt, pour 6,5 %, même si cette famille de ransomware a été active jusqu'en mai seulement. Les auteurs d'attaques par ransomware ont également affiné leurs cibles : leurs campagnes de phishing et d'ingénierie sociale visent des entreprises spécifiques ou des secteurs de l'industrie où le manque de disponibilité des données est très dommageable à leur activité...[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.



[Contactez-nous](#)



Réagissez à cet article

Original de l'article mis en page : Ransomware : une attaque
toutes les 40 secondes contre les PME – Le Monde Informatique