

# Quelles tendances en 2017 pour la sécurité du Cloud ?



Quelles tendances en 2017 pour la sécurité du Cloud ?

Comme chaque année, le grand jeu des prédictions des nouvelles tendances bat son plein. J'ai donc pris le parti de vous proposer quelques réflexions portant sur le marché du Cloud et celui de la sécurité en m'appuyant sur les dernières évolutions que j'ai pu constater.

### Les menaces inhérentes à l'IoT obligent les nations à s'engager dans la lutte internationale contre le piratage

Après les incidents qui ont frappé des infrastructures critiques en France, aux États-Unis et en Ukraine cette année, et face aux risques de piratage des machines de vote électroniques, les administrations de nombreux pays ont décidé de prendre le problème du cybrespionnage à bras-le-corps. Si les États-Unis ont réussi, par le biais de négociations diplomatiques à huis clos, à faire baisser le nombre d'attaques informatiques de la Chine à l'encontre des entreprises du secteur privé, le piratage des objets connectés représente un enjeu d'une tout autre ampleur. Sur le plan de la défense, l'Union européenne a adopté des dispositions législatives appelant à un minimum de mesures de cybersécurité pour protéger les infrastructures névralgiques, et les États-Unis devraient lui emboîter le pas en 2017.

### Des réglementations strictes influent sur la politique de cybersécurité des entreprises.

Les lois sur la protection de la vie privée des consommateurs sont censées avoir un effet dissuasif et sanctionner les négligences sécuritaires entraînant une violation de données. Or, jusqu'à présent, les organismes de réglementation semblent s'être bornés à de simples réprimandes. Sous l'impulsion de l'Europe et du nouveau règlement général sur la protection des données (GDPR), les autorités chargées de la protection des données redoublent de vigilance et reviennent le montant des amendes à la hausse. L'importance des sanctions financières infligées fin 2016 pour violation de la réglementation HIPAA et des directives de l'UE relatives aux données à caractère personnel donnent le ton pour l'année à venir. Nul doute que l'entrée en vigueur du GDPR en 2018 incitera les entreprises internationales à instaurer des contrôles supplémentaires pour la protection de la confidentialité.

**Les compromissions de données touchant des fournisseurs de services Cloud sensibilisent les entreprises aux risques de la « toile logistique ».** Le Cloud a transformé la chaîne logistique traditionnelle en « toile logistique » où les partenaires commerciaux échangent des données via des passerelles numériques sur Internet. Une entreprise moyenne traite avec 1 555 partenaires commerciaux différents via des services Cloud, et 9,3 % des fichiers hébergés dans le Cloud et partagés avec l'extérieur contiennent des données sensibles. Dans la nouvelle économie du Cloud, les données passent entre les mains d'un nombre d'intervenants plus élevé que jamais. Une violation de données peut ainsi toucher le partenaire externe d'une entreprise dont le département informatique et le service Achats n'ont jamais entendu parler.

### Restructuration des directions informatiques avec la promotion des RSSI

Avec l'avènement de la virtualisation, les technologies de l'information occupent une place tellement stratégique au sein de l'entreprise que les DSIs endossent désormais le rôle de directeur de l'exploitation et de PDG. En 2017, la sécurité s'imposera en tant que moteur d'activité stratégique, aussi bien au niveau des systèmes internes que des produits. Aujourd'hui, toutes les entreprises utilisent des logiciels, ce qui fait qu'elles ont besoin de l'expertise de fournisseurs de sécurité logicielle. En 2017, la sécurité confirmera son rôle d'autant concurrentiel en aidant les RSSI à réduire les délais de commercialisation des produits, et à assurer la confidentialité des données des clients et des employés.

### Microsoft réduira l'écart avec Amazon dans la guerre des offres IaaS

AWS s'est très vite imposé sur le marché de l'IaaS, mais Azure rattrape son retard. 35,8 % des nouvelles applications Cloud publiées au 4e trimestre ont été déployées dans AWS, contre 29,5 % dans Azure. Les fournisseurs spécialisés se sont taillé 14 % de parts de marché, indépendamment de marques telles que Google, Rackspace et Softlayer.

### Qui protège les gardiens ? Une entreprise sera victime du premier incident de grande ampleur dans le Cloud lié au piratage d'un compte administrateur

En fin d'année, des chercheurs ont, pour la première fois, découvert la mise en vente de mots de passe d'administrateurs Office 365 globaux sur le Dark Web. Les comptes administrateur représentent un risque particulier dans le sens où ils disposent de priviléges supérieurs en matière de consultation, de modification et de suppression des données. Les entreprises rencontrent en moyenne 3,3 menaces de sécurité liées à des utilisateurs privilégiés tous les mois. Nous devons par conséquent nous attendre à voir un incident de ce type faire la une des journaux en 2017.

### Les pirates délaissent les mots de passe au profit de la propriété intellectuelle

Maintenant que les entreprises ont toute confiance dans le Cloud et se servent d'applications SaaS pour les plans de produits, les prévisions de ventes, etc., les cybercriminels disposent de données de plus grande valeur à cibler. 4,4 % des documents exploités dans les applications de partage de fichiers sont de nature confidentielle et concernent des enregistrements financiers, des plans prévisionnels d'activité, du code source, des algorithmes de trading, etc. Si le piratage de bases de données comme celles de Yahoo se distinguent par leur ampleur, les secrets industriels représentent une manne d'informations plus restreinte, mais néanmoins précieuse. Pour répondre aux inquiétudes sur la confidentialité des informations hébergées dans le Cloud, des fournisseurs tels que Box établissent une classification des données permettant d'identifier les ressources qui revêtent le plus de valeur pour les entreprises...[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 JACOPPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».  
• Audits Sécurité (ISO 27001) ;  
• Expertises techniques et Judiciaires (avis techniques et judiciaires de preuves téléphones, disques durs, e-mails, commenteur, détournement de clientèle...) ;  
• Expertises de systèmes de sécurité électronique ;  
• Investigations et expertises en cybercriminalité ;  
• Formation au RGPD (Règlement Européen sur la Protection des Données) et au CIL (Correspondant Informatique et Libertés) ;  
• Accompagnement à la mise en conformité CNIL de votre établissement.



[Contacter-nous](#)

Réagissez à cet article

Original de l'article mis en page : Sécurité du Cloud : quelles tendances en 2017 ? – Globb Security FR

# 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

**A. L'exception des grands groupes, les entreprises françaises sous-estiment les risques de cyber-attaque** : moins de 4 sur 10 d'entre elles déclarent considérer comme « important », ou « très important », le risque que leur société subisse une cyber-attaque ces prochaines années, et ce, alors que 52% des entreprises ont déjà été piratées. C'est ce que montre une enquête réalisée par le cabinet Deloitte à l'Association en partenariat avec Sopra.

Les déclairs d'entreprises se font de fausses idées sur la cyber-fraude. Plus de trois sur quatre sous-estiment la vitesse de propagation de ce fléau dans l'Hexagone, pensant que le nombre des cyber-fraudes recensées en France n'a augmenté « que » de 10% ou de 20% en 2015, alors qu'il a triplé de 50% ! (Source : Anssi, Agence nationale de sécurité des systèmes d'information). Questionnés sur les cibles visées en priorité par les pirates, 50% des déclarés citent les multinationales ; ce pour 29% des répondants, les organismes publics constituent le premier choix des hackers. Seulement 20% des personnes interrogées connaissent la bonne réponse : les PME concentrant dans notre pays près de 80% des cyber-attaques (source : Sopra).

**Globallement, 70% des entreprises s'estiment bien protégées contre la cyber-fraude.** Une statistique qui recouvre des disparités : 38% des grands groupes affirment leur confiance dans leurs process de cybersécurité, tandis que 58% des TPE et environ 75% des PME et des ETI se jugent bien protégées.

**Quelles bonnes pratiques ?** Les entreprises ayant adopté une politique de cybersécurité ont mis en place, en moyenne, trois bonnes pratiques. Les plus répandues sont le changement régulier des codes d'accès à un réseau (réponse existant dans 50% des structures), et l'instauration en son sein d'une procédure d'authentification de tous les ordinateurs et commutateurs (50% des entreprises). La formation interne aux enjeux et aux risques de la cybersécurité, et la création de différents degrés d'accès au réseau pour les collaborateurs selon leur niveau hiérarchique (respectivement pratiquées par 40% et 44% des sociétés) se disloquent la troisième place sur le podium. Deux entreprises sur trois comptent adopter en 2017 de nouvelles mesures pour lutter contre le piratage informatique qui se décompose comme l'indique l'infographie ci-dessous.

**Quelles nouvelles mesures de cybersécurité prévoit-on d'adopter en 2017 ?**

Augmenter le niveau de sensibilisation et de formation à la cybersécurité	37%
mettre en place un système d'alerte et de réponse	30%
mettre en place des codes d'accès à un réseau	29%
mettre en place une procédure d'authentification	19%
mettre en place une politique de cybersécurité	17%
mettre en place une politique de sécurité et de gestion des données	17%
mettre en place une protection du matériel	15%
mettre en place une protection de l'information	15%
mettre en place une protection de l'information et de l'outil	14%
autre mesure prévue	10%
aucune mesure prévue	2%

90% des entreprises françaises sont disposées à investir chaque année pour se protéger efficacement contre la cyber-fraude, et 60% sont même prêtes à y consacrer un budget supérieur ou égal à 1% de leur chiffre d'affaires. Parmi les différentes catégories d'entreprises, les PME et les ETI se montrent les plus enclines à réaliser un effort financier conséquent : les trois-quarts d'entre elles acceptent de dépasser chaque année pour leur cybersécurité entre 2% et 6% de leur chiffre d'affaires.

Si l'on exclut les entreprises de très petites structures, peu ou pas du tout concernées par ces sujets, les déclarés apparaissent bien conscients des nouveaux risques encourus par les entreprises, et décidés à les combattre. En effet, 60% des décideurs indiquent qu'ils se préoccupent au cours des trois années à venir de lutter contre les « ransomwares » ; 70% disent qu'ils s'attacheront à sécuriser les données mises sur le cloud ; et 70% déclarent qu'ils veilleront à prévenir les risques liés aux objets connectés.

Original de l'article mis en page : Les entreprises françaises sous-estiment les risques de cyber-attaque

**Notez-moi !** : Vous aidez à vous protéger des pirates informatiques (attaque, arnaque, cryptovirus) et vous assistez 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'aide dans toute la France et à l'étranger, nous répondons aux préoccupations des déclarés 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).

Plus d'informations sur : <http://www.le-net-expert.com/formation-cybersecurite-protection-des-donnees-personnelles>



**Le Net Expert**  
INFORMATIQUE  
CYBERSECURITE  
CONSULTANT EN CYBERSECURITE

[Découvrez à cet article](#)

# Tendances émergentes actuelles pour la cybersécurité en 2017 et la



**Denis JACOPINI**  
EXPERT INFORMATIQUE ADOPTÉE SPÉCIALE EN CYBERCRIMINALITÉ

**vous informe**

**Tendances actuelles 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

# Un raccourci Windows qui peut flinguer votre sécurité



Un raccourci Windows qui peut flinguer votre sécurité

**Un chercheur Français découvre comment il est possible de télécharger et exécuter n'importe quel fichier en utilisant un outil natif de Windows. Une porte ouverte pour des infiltrations malveillantes.**

Notre ami Jean-Pierre LESUEUR, le fondateur de Phrozen software n'est plus à présenter. Ce chercheur en sécurité informatique, auteur de nombreux logiciels permettant de contrer pirates et codes malveillants vient de trouver une petite finesse dans l'ensemble des Windows, et cela à partir du SP2 de Windows XP qui risque de faire réagir rapidement le géant américain. Le problème est simple, à travers un raccourci Windows, il est possible de télécharger et exécuter n'importe quel fichier en utilisant un outil natif de Windows. « **Du coup forcement**, explique Jean-Pierre Lesueur, *indétectable par les Antivirus actuels car un raccourci n'est pas directement un fichier exécutable*» .

Seulement, cette première découverte a fait suite à une seconde 100 fois plus vicieuse encore. Réussir à injecter une application directement dans le raccourci, ainsi plus besoin de télécharger et exécuter le code malveillant. Bilan, les pare-feu ne risquent plus de bloquer la potentielle attaque. Bref, une nouvelle couche problématique...[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 : ZATAZ Quand un raccourci Windows peut flinguer votre sécurité – ZATAZ

---

# 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 débloquer 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 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 débloquer 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 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>Denis JACOPINI vous informe</p>	<p>Pourquoi les DSI sont-ils inquiets à l'approche des Fêtes de fin d'année ?</p>
--	---

**La dernière étude dIFS 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.

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**

Denis JACOPINI



**vous informe**

**Rakos, un nouveau botnet qui vise aussi les objets connectés**

**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

# Le RGPD règlement européen de protection des données et les contrats fournisseurs



Denis JACOPINI  
VOUS INFORME

Le règlement européen de protection des données et les contrats fournisseurs

RDPD , de des tes

**Entré en vigueur en mai dernier, le Règlement général sur la protection des données impose de nouvelles règles en matière de gestion des données personnelles. Avec l'obligation pour les entreprises de se mettre en conformité avant mai 2018. Ce qui implique une modification des contrats fournisseurs.**

#### **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.

#### **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 fournisseurs et clients sont impactés (voir encadré ci-dessous).

« 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 responsabilités en fonction de la mainmise de chacun sur les données. Cette notion de coresponsabilité doit être intégrée dès maintenant dans les contrats passés avec les fournisseurs: en effet, le sous-traitant désigné par une organisation pour assurer le traitement des données devient, avec le RGPD, coresponsable de la légalité des traitements. Il sera donc tenu d'informer ses clients et de tenir des registres pour recenser les données, ainsi que d'accepter les audits demandés par son client pour s'assurer de la conformité des traitements. Les sous-traitants concernés peuvent être, par exemple, l'éditeur d'un CRM en ligne, le routeur d'une campagne d'e-mailing, un service de relation client, etc. Le responsable du traitement, de son côté, doit s'assurer que ses fournisseurs ont pris les mesures nécessaires pour assurer la sécurité des 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. Quel impact sur les contrats fournisseurs? Pour se mettre en conformité avec le RGPD, les directeurs achats devront veiller à renforcer les contrats passés avec leur fournisseurs...[lire la suite]

**Notre métier :** Vous accompagner dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

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

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



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 DRETEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

# 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 vérifiées 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 vielle 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 téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Avis technique et octet n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Liberté) ;
- 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