# Près de la moitié des Français confrontés à la cybercriminalité


Près de la moitié des Français confrontés à la cybercriminalité

---

**Ransomware ou vol des données bancaires : près d'un Français sur deux (47%) a déjà été victime de cybercriminalité au cours de sa vie, selon l'étude annuelle Norton/Symantec révélée par Le Parisien / Aujourd'hui en France.**


La cybercriminalité touche plus particulièrement les Français, puisque seulement quatre Européens sur dix sont confrontés à ce phénomène.
En détail, plus d'un Français sur dix (12%) déclare avoir été victime d'un ransomware, un logiciel malveillant qui permet au cybercriminel de demander de l'argent aux utilisateurs en échange de la décontamination de leur ordinateur, alors que 20% des Français confient avoir été victimes du vol de leurs données bancaires.
Ce rapport montre que les Français sont particulièrement méfiants vis-à-vis de la cybercriminalité. Plus de la moitié des sondés (55%) ont aujourd'hui plus peur de se faire voler leurs données bancaires en ligne que de se faire subtiliser leur portefeuille.
Plus de 17.000 consommateurs dans le monde ont été sondé cet automne pour les besoins de cette étude.

---

Réagissez à cet article
Source : http://www.lejdc.fr/france-monde/actualites/societe/techno/2015/11/30/pres-de-la-moitie-des-francais-confrontes-a-la-cybercriminalite_11685497.html

---

# 12 % des entreprises belges victimes d'attaques

# informatique…| Le Net Expert Informatique


## 12 % des entreprises belges victimes d'attaques informatique…

**Quelque 12% des PME belges ont déjà été confrontées au moins une fois à une attaque par déni de service, également appelée DDoS, suivies de près (11%) par les PME plus petites ou unipersonnelles.**

Les entreprises de plus grande taille obtiennent, quant à elles, un résultat légèrement meilleur, avec 9%, ressort-il mercredi d'une étude de Kaspersky Lab, société spécialisée dans la sécurité des systèmes d'information. Au niveau mondial, un quart des attaques a entraîné la perte de données sensibles.

De telles attaques visent à rendre un serveur, un service ou une infrastructure indisponibles en surchargeant la bande passante du serveur ou en accaparant ses ressources jusqu'à épuisement.

Le coût pour tout rétablir peut aller jusqu'à 367.000 euros. «En moyenne, une attaque DDoS coûte aux organisations plus de 40.000 euros en factures de restauration. Les grandes entreprises dépensent des montants encore supérieurs à la récupération après une perturbation externe ou attaque de cyber-espionnage. L'investissement moyen après une attaque DDoS s'élève ainsi à environ 367.000 euros contre les 546.000 euros dépensés en moyenne par ces entreprises pour se remettre d'autres formes d'attaques», détaille l'étude 'Corporate IT Security Risks Survey', réalisée par Kaspersky Lab et B2B International auprès de 5.500 entreprises à travers le monde.

Au niveau mondial, 9% des attaques qui paralysent un service durent de deux jours à une semaine et, dans 7% des cas, ce type d'attaque dure plusieurs semaines ou davantage. Mais les dommages ne se limitent pas au temps d'arrêt: ils peuvent également perturber totalement les activités des entreprises et provoquer, pour environ 7% des PME sondées, la perte de données confidentielles.

---

Comme tout professionnel de l'informatique et de l'Internet, il est de mon devoir de vous informer que vous devez mettre en conformité et déclarer à la CNIL tous vos traitement de données à caractère personnel (factures, contacts, emails…).

Même si remplir un formulaire de déclaration à la CNIL est simple et gratuit, il vous engage cependant, par la signature que vous apposez, à respecter point par point la loi Informatique et Libertés. Cette démarche doit commencer par une analyse précise et confidentielle de l'ensemble de vos systèmes de traitements de données. Nous pouvons vous accompagner pour vous mettre en conformité avec la CNIL, former ou accompagner un C.I.L. (correspondant CNIL) ou sensibiliser les agents et salariés à l'hygiène informatique.

Besoin d'informations complémentaires ?

Contactez-nous

Denis JACOPINI
Tel : 06 19 71 79 12
formateur n°93 84 03041 84

---

Denis JACOPINI est Expert Informatique assermenté, consultant et formateur en sécurité informatique, en mise en conformité de vos déclarations à la CNIL et en cybercriminalité.

Nos domaines de compétence :

• **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;

• **Consultant** en sécurité informatique, cybercriminalité, en accompagnement aux mises en conformité et déclarations à la CNIL ;

• **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL et accompagnement de Correspondant Informatique et Libertés.

Contactez-nous

---

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : http://www.lavenir.net/cnt/dmf20151028_00726712

# Usages et statistiques d’Internet dans le monde | Le Net Expert Informatique


## Usages et statistiques d’Internet dans le monde

Le septembre 28, 2015 à 12h00Utilisateurs Internet dans le monde : 3 213 216 044
Nombre total de cyber attaques ce jour : 12 562 128
Recherches Google cette année 615 581 599 674
E-mails envoyés ce jour 122 536 516 003
E-mails envoyés cette année  79 309 569 450 691
Téléphones mobiles en service dans le monde : 5 574 565 107
Cartes SIM actives dans le monde : 8 700 569 273
Nombre Total de téléphones Android dans le monde : 3 961 847 660
Sites Web ayant été piraté cette année : 77 916
Les menaces en ligne ce mois dans le monde : 82 394 168
Téléphones mobiles vendus ce jour : 3 135 027
Lire la suite….

---

Denis JACOPINI est Expert Judiciaire en Informatique, consultant, formateur et chargé de cours.
Nos domaines de compétence :

- **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
- **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
- **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.

Contactez-nous

---

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : https://kaspersky-cyberstat.com/fr/

# Le vol d’identité en tête des attaques en cybercriminalité | Le Net Expert Informatique


## Le vol d’identité en tête des attaques en cybercriminalité

**Selon l'étude Breach Level Index pour le premier semestre 2015 publié par le leader mondial de la sécurité numérique Gemalto, il apparaît 888 failles de données signalées au cours de cette période, compromettant ainsi 246 millions d'enregistrements de données dans le monde.**

Les failles de sécurité ont augmenté de 10 % par rapport au premier semestre de l'année précédente, alors que le nombre d'enregistrements de données compromis diminuait de 41 % au cours des six premiers mois. Cette nette amélioration peut être attribuée à la diminution du nombre de méga-failles à très grande échelle ayant touché le commerce de détail et la distribution, comparativement à la même période de l'année écoulée.

Malgré la diminution du nombre de données compromises, les failles les plus importantes ont touché des volumes considérables d'informations personnelles. L'incident le plus important constaté au cours du premier semestre – niveau 10 sur l'échelle de gravité du Breach Level Index –, a concerné un vol d'identité dont a été victime l'assureur-santé Anthem Insurance aux États-Unis, qui a impacté 78,8 millions de fichiers, soit le tiers (32 %) de l'ensemble des fichiers de données volés au cours du premier semestre. Parmi les autres failles notables recensées au cours de la période d'analyse, il faut citer une attaque touchant 21 millions de fichiers de l'US Office of Personnel Management (9,7 sur l'échelle BLI) ; une attaque touchant 50 millions de fichiers de la Direction générale de la population et des affaires de la citoyenneté en Turquie (9,3 sur l'échelle BLI) ; et une défaillance affectant 20 millions de fichiers du site de rencontre russe Top Face (9,2 sur l'échelle BLI). Les dix principales cyber-attaques ont représenté 81,4 % de l'ensemble des fichiers compromis.

« Nous sommes obligés de constater le fort retour sur investissement des attaques sophistiquées que mènent les hackers, qui affectent des volumes considérables de données. Les cybercriminels continuent de s'approprier, la majeure partie du temps en toute impunité, des jeux de données extrêmement précieux. A titre d'exemple, les failles qui ont touché le secteur de la santé au cours du premier semestre leur ont permis de recueillir en moyenne plus de 450 000 fichiers de données, soit une augmentation de 200 % par rapport à la même période de 2014 », explique Jason Hart, vice-président et directeur de la technologie, en charge du pôle protection des données chez Gemalto.

**Incidents par source**

Le nombre d'attaques conduites à l'instigation ou avec la bénédiction d'un État ou d'un service gouvernemental n'ont représenté que 2 % de l'ensemble des incidents enregistrés. Le nombre de fichiers affectés par ces épisodes représente toutefois 41 % de l'ensemble des fichiers compromis, en raison notamment de l'attaque ayant ciblé Anthem Insurance et l'US Office of Personnel Management. Alors qu'aucune des dix principales failles enregistrées au premier semestre 2014 n'était le résultat d'une action soutenue par un État, trois des principaux incidents recensés cette année ont été menés à l'instigation de services gouvernementaux et notamment les deux premiers en termes de sévérité.

Les intrusions malveillantes menées à titre individuel ont cependant été la principale cause des failles de données enregistrées au premier semestre 2015, représentant 546 ou 62 % des attaques informatiques, contre 465 ou 58 % au premier semestre de l'année écoulée. 116 millions (soit 46 %) des fichiers affectés globalement l'ont été en raison d'intrusions malveillantes, ce qui constitue un net recul sur les 298 millions d'incidents (71,8 %) répertoriés en 2014.

**Incidents par type**

Le vol d'identité demeure, au premier semestre, la principale cible des cybercriminels, représentant 75 % de tous les fichiers affectés, et un peu plus de la moitié (53 %) des failles de données enregistrées. Cinq des dix principales failles, y compris les trois premières – toutes trois classées au niveau « catastrophique » sur l'échelle BLI –, ont porté sur des vols d'identité, contre sept sur dix au cours du premier semestre 2014.

**Incidents par secteur**

De tous les domaines d'activité recensés, les secteurs gouvernementaux et de la santé ont payé le plus lourd tribut à la cybercriminalité, puisqu'ils représentent environ les deux tiers (31 % et 34 % respectivement) des fichiers de données compromis. La santé ne représente toutefois que 21 % des atteintes informatiques enregistrées cette année, contre 29 % au cours du premier semestre de l'année précédente. Le secteur du commerce de détail et de la distribution connaît une nette diminution du nombre de fichiers volés, représentant seulement 4 %, contre 38 % au cours de la même période de l'année écoulée. En termes de localisation géographique, les États-Unis sont le pays le plus touché, avec plus des trois quarts (76 %) des failles de données enregistrées, et près de la moitié (49 %) de l'ensemble des fichiers affectés par des attaques. La Turquie représente 26 % des compromissions de données, avec notamment une attaque massive ciblant la Direction générale de la population et des affaires de la citoyenneté, au cours de laquelle quelque 50 millions de fichiers numériques ont été forcés dans le cadre d'une intrusion malveillante.

Le niveau de chiffrement utilisé pour protéger les données exposées – capable de réduire considérablement le nombre et l'impact des failles de données –, a légèrement augmenté et se situe à 4 % pour toutes les attaques enregistrées, contre 1 % au cours du premier semestre 2014.

« Malgré la fluctuation du nombre de failles de données, la question reste la même : il ne s'agit pas de savoir 'si' vous allez être victime d'un vol de données, mais 'quand'. Les données collectées dans le cadre de l'étude Breach Level Index montrent que la majeure partie des sociétés ne sont pas en mesure de protéger leurs données dès lors que leur défense périmétrique a été mise à mal. Alors même qu'un nombre croissant d'entreprises procèdent à un chiffrement de leurs données, elles ne le font pas au niveau requis pour réduire l'ampleur et la gravité de ces attaques », explique Jason Hart. « Les entreprises doivent adopter une vision de la menace numérique centrée sur les données, à commencer par l'instauration de techniques de gestion des identités et de contrôle d'accès beaucoup plus efficaces, qu'il s'agisse de procédures d'authentification multifactorielle ou du chiffrement des données, pour rendre inutilisables les informations dérobées. »

Selon le cabinet Forrester, l'habileté et la sophistication croissantes des cybercriminels se traduisent par une érosion de l'efficacité des contrôles et techniques de sécurité classiques, essentiellement basées sur un contrôle périphérique. La mutation constante du paysage de la cybercriminalité nécessite donc de nouvelles mesures défensives, avec notamment la généralisation des technologies de chiffrement. Dans l'avenir, les sociétés procéderont par défaut à un chiffrement dynamique de leurs données, mais aussi lorsque leurs systèmes et leurs données seront au repos. Cette approche de la sécurité centrée sur les données s'avère beaucoup plus efficace pour lutter contre des cybercriminels déterminés. En adoptant le chiffrement des données sensibles, qui les rend inutilisables, les sociétés incitent les cybercriminels à aller chercher des cibles beaucoup moins bien protégées. Le chiffrement est appelé à devenir la clé de voûte de la sécurité informatique. Ce sera donc un élément stratégique central pour les responsables de la sécurité et de la gestion des risques au sein des entreprises.

---

Denis JACOPINI est Expert Judiciaire en Informatique, consultant, formateur et chargé de cours.
Nos domaines de compétence :
• **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
• **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
• **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.
Contactez-nous

---



Source : http://afriqueinside.com/securite-numerique-les-vols-didentite-en-tete-de-la-cybercriminalite09092015/

# La Cybercriminalité est rentable | Le Net Expert Informatique

## La Cybercriminalité est rentable

**Selon l'édition du 1er semestre 2015 du Breach Level Index (BLI) de Gemalto, 246 millions d'enregistrements ont été compromis au cours de la période étudiée en raison de 888 failles. La cybercriminalité majoritaire (53% des failles) reste les vols d'identité.**

62% des attaques informatiques (contre 58% sur la période précédente) restent des attaques individuelles. Si les atteintes émanant d'un Etat ou d'un service gouvernemental représentent 2% du nombre des incidents, elles constituent 41% des volumes de données compromises, surtout à cause de deux gros incidents (Anthem Insurance, avec 78,8 millions d'enregistrements compromis soit 32% du total à lui seul, et US Office of Personnel Management). Les dix principales attaques ont représenté 81,4% de l'ensemble des volumes compromis. Les Etats-Unis ont représenté 76% des failles et 49% des volumes compromis.

**Des évolutions contrastées**

Le volume de données compromises a baissé de 41% par rapport à la période précédente mais les failles de sécurité ont, elles, augmenté de 10%. Les failles, aujourd'hui, sont moins des méga-failles frappant de nombreux systèmes qu'auparavant, ce qui explique cette évolution contrastée. Gemalto ne peut que constater la grande rentabilité des activités cybercriminels, tant l'impunité est la règle et la valeur des données compromises importante.

Les deux-tiers des compromissions concernent le secteur public (31%) et celui de la santé (34%). Le nombre d'attaques contre le secteur de la santé a cependant baissé par rapport à la période précédente, passant de 29% à 21%. Commerce de détail et distribution, qui étaient des victimes importantes, ne sont plus que marginales ce semestre (de 38% à 4%).

**A propos de l'étude**

Réalisé par Gemalto, le Breach Level Index (BLI) centralise les failles de données au sein d'une base de données mondiale et calcule leur gravité selon de multiples critères, parmi lesquels le type de données et le nombre d'enregistrements volés, la source de la faille, et le fait que les données aient été chiffrées ou non. En attribuant un score de gravité à chaque faille, le BLI dresse une liste comparative des failles, en distinguant les gênes des méga-failles réellement dangereuses. Les informations qui alimentent le référentiel BLI proviennent de données disponibles publiquement.

---



---



Source : http://www.cio-onli
ne.com/actualites/lire-cybersecurite%C2
%A0-le-crime-paie-et-est-rentable-7857.html
Par Franck Salien, Journaliste

# Les chiffres clés de l’Internet en France et dans le monde | Le Net Expert Informatique

Les chiffres clés de l'Internet

- Nombre internautes France
- Nombre internautes Europe
- Nombre mobinautes France
- Réseaux sociaux dans le monde
- Temps passé sur Facebook, Google et Microsoft
- Panier moyen e-commerce en France
- Marché de l'etourisme en France
- Marché de l'e-commerce aux US
- PDM des OS mobiles en France
- Nombre de cyberacheteurs France
- Nombre de sites marchands France
- Réseaux sociaux en Europe
- Services les plus utilisés
- Réseaux sociaux sur mobile
- PDM des moteurs dans le monde
- PDM des moteurs en France
- Marché de l'e-commerce en France
- Marché des navigateurs
- Nombre de SMS envoyés en France
- Marché de l'e-commerce dans le monde
- Abonnés mobile en France
- Marché de l'e-commerce au Royaume-Uni
- Transformation des sites marchands
- Typologie des sites marchands
- Marché de l'e-commerce en Allemagne
- Marché de l'e-pub en France
- Marché de l'e-commerce en Italie
- Réseaux sociaux dans le monde

---



---



---



Source : http://www.journaldunet.com/web-tech/chiffres-internet

# Les Chiffres et Statistiques du numérique : Usages, risques, cybercriminalité (Dernière infos rajoutées le 17/07/2015)

Dernière infos rajoutées le 17/07/2015

Dans le but de vous permettre de mieux juger l'importance du Risque Informatique et de la Cybercriminalité en France et ailleurs, nous avons souhaité mettre à disposition le résultat de nos collectes successives de statistiques relativement impressionnantes.

Ces chiffres ne m'appartiennent pas et pour chacun d'eux, est indiqué la date d'ajout dans ce document et la source d'information associée. Cependant, **si vous souhaitez reprendre tout ou partie du résultats de mes recherches, je vous demanderais soit de citer « Denis JACOPINI » ou « Le Net Expert » comme source de votre information**.

---

Besoin d’informations complémentaires ?

Contactez-nous

Denis JACOPINI
Tel : 06 19 71 79 12
formateur n°93 84 03041 84

---

Imaginez un instant que vous soyez consommateur. Vous découvrez soudain que vos données (coordonnées personnelles, bancaires ou encore médicales) se trouvent diffusées sur le net, sans votre accord, à cause de la négligence d’un professionnel.
Imaginez maintenant que ce professionnel c’est vous, et ce, malgré la mise en application imminente du projet de règlement Européen sur la Protection des données personnelles, le risque d’anéantir votre réputation et de vous sanctionner lourdement. Certes, le mal est fait mais pire, les Cybercriminels sauront en profiter !

---

Lorsque, lors de conférences, je m’adresse à des entreprises pour leur parler de sécurité informatique et de risque de piratage, les chefs d’entreprises, pourtant vêtus d’une responsabilité souvent pénale, me rétorquent du « On n’est pas concerné, on n’est pas la Nasa », du « On n’a pas de secret qui pourrait intéresser des pirates, on ne risque rien » ou bien du « de toute façon, le peu de contrôles que la CNIL fait n’aboutissent qu’à des amendes symboliques ».

De leur répondre : « Bien sur que si, vous avez des informations secrètes, et même ultra secrètes : LES DONNEES A CARACTERE PERSONNEL DE VOS CLIENTS ». Et vous avez même ente vos main quelque chose d’encore plus précieux que ça : VOTRE REPUTATION »

Trop peu respectée, la loi informatique et libertés fixe impose à tout responsable de traitement de données personnelles de mettre en place des mesures de sécurité appropriées à la protection des données à caractère personnel.

Sans cela, données non protégées = données piratées et diffusées dans la nature = risque pénal mais surtout réputation salie.

---

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement. Besoin d'informations complémentaires ?

Contactez-nous

Denis JACOPINI
Tel : 06 19 71 79 12
formateur n°93 84 03041 84

---

## INTERNET DANS LE MONDE EN 2014

42% de la population mondiale soit 3,025 milliards de personnes utilisent le réseau internet. (D27-S35)

Sur l'ensemble du continent africain, le taux de pénétration d'Internet est estimé à 16% en 2014 soit 167 millions d'internautes, contre 110 millions en 2010. (D27-S35)

Le nombre des utilisateurs d'Internet en Afrique devrait être

multiplié par 3.5 d’ici 2015 pour que le nombre d’internautes atteigne près de 600 millions. (D27-S35)

Nombre d’internautes : 3,001,769,770 (35% de la population mondiale). (D9-S16)

Le cap des 3,2 milliards d’internautes devrait être dépassé dans le monde en 2014

Taux de pénétration d’Internet dans le Monde :
81% en Amérique du Nord (86% au Canada, 80% aux USA) (D9-S16)
78% en Europe de l’Ouest (83% en France) (D9-S16) 18% en Afrique (D9-S16)
12% en Asie du Sud (D9-S16)
822 240 nouveaux sites Internet sont mis en ligne chaque jour (D9-S16)

Chaque minute sur Internet : (D9-S16)
2 millions de requêtes Google sont effectuées
347 nouvelles publications WordPress sont publiées
571 nouveaux sites web sont créés
2000 nouvelles photos sont ajoutés sur Tumblr
204 millions d’emails sont envoyés

---

**Denis JACOPINI est à l’origine de cette collecte d’information. Merci de le citer si vous utilisez le résultat de ce travail.**

**Denis JACOPINI est Expert Informatique assermenté et formateur spécialisé en mise en conformité avec la CNIL, en sécurité Informatique, en cybercriminalité et en protection des données à caractère personnel.**

Posez vos questions

## TÉLÉCHARGEMENT ILLÉGAL ET LOI HADOPI

10% des abonnés avertis une fois récidivent. (D23-S31)

Sur les 8,9% de titulaires d'un abonnement à Internet ayant reçu un premier avertissement (entre octobre 2010 et juin 2014, soit plus de 3,2 millions d'emails envoyés), ils ne sont plus que 10,4% d'entre eux à avoir été avertis une deuxième fois – puis 0,4% à s'être retrouvés en phase 3. (D23-S31)

70% diminuent leur consommation illicite après l'avertissement 1. (D23-S31)

88% diminuent leur consommation illicite après l'avertissement 2. (D23-S31)

Après un avertissement, seulement 23% à déclarer se tourner vers une offre légale. (D23-S31)

---

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement. Besoin d'informations complémentaires ?

Contactez-nous

Denis JACOPINI
Tel : 06 19 71 79 12
formateur n°93 84 03041 84

---

## LA SÉCURITÉ ET LES CERTIFICATS SSL

Jusqu’à 91% des internautes n’iront pas plus loin en cas d’avertissement au risque de malware ou de phising. (D17 – S25)

Plus des 2/3 (77%) des sites Internet propagateurs de malwares sont des sites légitimes infectés. (D17 – S25)

Un site Internet sur 8 comporte des vulnérabilités critiques. (D17 – S25)

---

**Denis JACOPINI est à l’origine de cette collecte d’information. Merci de le citer si vous utilisez le résultat de ce travail.**

**Denis JACOPINI est Expert Informatique assermenté et formateur spécialisé en mise en conformité avec la CNIL, en sécurité Informatique, en cybercriminalité et en protection des données à caractère personnel.**

Posez vos questions

---

## LES FRANCAIS ET LE PAIEMENT SANS CONTACT NFC

15 % utilisent la fonction NFC de leur CB (D24-S32)

19 % ignorent si leur carte dispose de cette option (D24-S32)

34% estiment cette technologie utile (D24-S32)

22% des Français sont à l'aise avec le paiement sans contact (D24-S32)

44 % ont connaissance de la fonction paiement sans contact de leur carte bancaire (D24-S32)

29 % ne s'en servent pas sachant qu'ils ont cette option (D24-S32)

---

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être

personnalisées et organisées dans votre établissement.
Besoin d’informations complémentaires ?

Contactez-nous

Denis JACOPINI
Tel : 06 19 71 79 12
formateur n°93 84 03041 84

---

## LA SÉCURITÉ ET LE BYOD

95% des entreprises se disent menacées par des problèmes de sécurité liés au BYOD. (D17-S24)

82% pensent même que le nombre d’incidents dans ce domaine va croître en 2015 par rapport à 2014. (D17-S24)

47% des entreprises ont éprouvé des intrusions suite à des brèches présentes dans des appareils mobiles. (D17-S24)

64% pensent qu’Android est toujours considéré comme le système d’exploitation le plus risqué des OS mobiles. (D17-S24)

---

**Denis JACOPINI est à l’origine de cette collecte d’information. Merci de le citer si vous utilisez le résultat de ce travail.**

**Denis JACOPINI est Expert Informatique assermenté et formateur**

**spécialisé en mise en conformité avec la CNIL, en sécurité Informatique, en cybercriminalité et en protection des données à caractère personnel.**

Posez vos questions

---

## LA SÉCURITÉ EN ENTREPRISE

Une étude internationale a interrogé 450 décideurs informatiques et révèle que de nombreuses sociétés se heurtent aux exigences de gouvernance et de sécurité des échanges de données. (D22-S30).

23% des entreprises ont récemment échoué à un audit de sécurité, tandis que

17 % doutent de leur capacité à réussir un audit de conformité des échanges de données.

Le coût total moyen d'une atteinte à l'intégrité des données s'élève à 2,4 millions d'euros.

La stratégie d'intégration n'est pas alignée avec les structures et les politiques de gouvernance, de confidentialité et de sécurité des données pour 71% des entreprises.

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement. Besoin d'informations complémentaires ?

Contactez-nous

Denis JACOPINI
Tel : 06 19 71 79 12
formateur n°93 84 03041 84

---

## LA CYBERCRIMINALITE ET LES MOBILES

Entre janvier et juin 2014, le nombre d'infections touchant les terminaux mobiles a progressé de 17% (20% seulement sur tout 2013. (D15-S22)

0,65% des smartphones en circulation sont infectés d'un malware. Les smartphones équipés d'Android comptent 60% des équipements mobiles infectés contre 40% pour les PC portables équipés de Windows.

De leur côté, les iPhone, les BlackBerry, les téléphones sous Symbian et sous Windows Phone totaliseraient moins de 1%.

Le cheval de Troie *Android.Trojan.Coogos.A!tr* représenterait 35,69% des attaques ciblant Android.

---

**Denis JACOPINI est à l'origine de cette collecte d'information. Merci de le citer si vous utilisez le résultat de ce travail.**

**Denis JACOPINI est Expert Informatique assermenté et formateur spécialisé en mise en conformité avec la CNIL, en sécurité Informatique, en cybercriminalité et en protection des données à caractère personnel.**

Posez vos questions

---

## LE CLOUD EN ENTREPRISE

Enquête Eurostat : Utilisation des TIC dans les entreprises en 2014 (D19-S21)

19% des entreprises utilisait des services de cloud computing en 2014

45%  secteur de l'information & de la communication

27% activités spécialisées, scientifiques et techniques

14% et 20% dans tous les autres secteurs économiques

Pour les 81% des entreprises n'utilisant pas le cloud, une connaissance insuffisante de ces services informatiques constituait le principal facteur bloquant.

En 2014, les proportions les plus élevées d'entreprises

utilisant le cloud ont été observées en Finlande (51%), en Italie (40%), en Suède (39%) ainsi qu'au Danemark (38%). À l'opposé, les services de cloud computing étaient utilisés par moins de 10% des entreprises en Roumanie (5%), en Lettonie et en Pologne (6% chacun), en Bulgarie, en Grèce et en Hongrie (8% chacun).
Dans seize États membres, le cloud était principalement utilisé pour les services de courrier électronique, notamment en Italie (86%), en Croatie (85%) et en Slovaquie (84%). Les services de cloud computing étaient principalement utilisés pour le stockage de fichiers dans onze autres États membres, les proportions les plus élevées ayant été observées en Irlande (74%), au Royaume-Uni (71%), au Danemark ainsi qu'à Chypre (70% chacun), tandis que l'hébergement de la base de données de l'entreprise était l'usage du cloud le plus courant aux Pays-Bas (64%).

Enquête Unitrend auprès d'entreprises (D19-S21) :

78% ont connu des coupures des applications critiques.

63% estiment que les pertes ainsi engendrées vont de quelques centaines de dollars à plus de 5 millions.

28% des entreprises touchées par un incident estiment que leurs entreprises ont été privées de fonctions clés de leurs datacenters pendant des périodes pouvant aller jusqu'à plusieurs semaines.

73% des entreprises déclarent ne pas prêtes pour la restauration après sinistre.

60% estiment qu'elles n'ont pas complètement documenté leur plan de reprise d'activité.

23% n'ont jamais testé ces plans de reprise d'activité.

---

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement. Besoin d'informations complémentaires ?

Contactez-nous

Denis JACOPINI
Tel : 06 19 71 79 12
formateur n°93 84 03041 84

---

## CE QUE PENSENT LES ENTREPRISES DE LEUR SECURITÉ

Sept entreprises sur dix seraient  convaincues de disposer d'un pare-feu de nouvelle génération (*Next Generation Firewall*, ou NGFW) alors que… non, elles ne seraient en fait que 30 % à en posséder. (D16-S23)

54 % des DSI français pensent que leur pare-feu dispose de capacités de détection avancées efficaces, intégrant notamment des fonctions de sandboxing spécifiques aux fameux NGFW. (D16-S23)

31 % des décideurs IT estiment que leur entreprise utilise trop de solutions de sécurité pour gérer les menaces. (S16-S23)

**Denis JACOPINI est à l'origine de cette collecte d'information. Merci de le citer si vous utilisez le résultat de ce travail.**

**Denis JACOPINI est Expert Informatique assermenté et formateur spécialisé en mise en conformité avec la CNIL, en sécurité Informatique, en cybercriminalité et en protection des données à caractère personnel.**

Posez vos questions

---

## LE DROIT À L'OUBLI

Les plaintes liées au droit à l'oubli, en hausse de quatre points par rapport à 2012, ont représenté 34 % du nombre total de plaintes en 2013. (D13-S20)

---

**Denis JACOPINI est à l'origine de cette collecte d'information. Merci de le citer si vous utilisez le résultat de ce travail.**

**Denis JACOPINI est Expert Informatique assermenté et formateur spécialisé en mise en conformité avec la CNIL, en sécurité Informatique, en cybercriminalité et en protection des données à caractère personnel.**

Posez vos questions

---

## CYBERCRIMINALITÉ

5 entreprises sur 6 employant plus de 2 500 personnes ont été la cible de cyberattaques en 2014 (D28-S36)

Entre 2013 et 2014, le nombre des cyberattaques a augmenté de 120% dans le monde et le coût estimé de la cybercriminalité pour les entreprises s'élève en moyenne à 7,6 millions de dollars par an, soit une augmentation de 10% (D26-S34)

61 % des victimes d'une attaque DDoS ont temporairement perdu l'accès à des informations critiques (D25-S33)

38 % ont été dans l'incapacité de poursuivre leur activité principale(D25-S33)
33 % font état de pertes d'opportunités et de contrats (D25-S33)
Dans 29 % des cas, le succès d'une attaque DDoS a eu un impact négatif sur la cote de crédit de l'entreprise (D25-S33)
Dans 26 % des cas, a entraîné une augmentation de ses primes d'assurance (D25-S33)
A la suite d'une attaque DDOS, 49 % ont payé pour faire modifier leur infrastructure informatique, 46 % ont eu recours à leurs avocats et 41 % ont fait appel à des gestionnaires de risque (D25-S33)

72 % des victimes ont divulgué des informations relatives à une attaque DDoS contre leurs ressources. En particulier, 43 % des responsables interrogés ont informé leurs clients d'un incident, 36 % l'ont signalé aux autorités et 26 % en ont parlé aux médias. 38 % des entreprises ont subi une atteinte à leur réputation à la suite d'une attaque DDoS et près d'une sur trois a dû demander l'aide de conseillers en image (D25-S33)

48 % des attaques cibleraient directement des applications web des e-commerçants. (D20-S28)

40 % des attaques par injection SQL et 64 % des campagnes de trafic http malveillant concernent les sites de commerce en ligne. (D20-S28)

Selon l'enquête d'Imperva, les sites de commerce en ligne sont attaqués deux fois plus souvent que des sites plus classiques. Les attaques durent aussi plus longtemps : près de deux fois plus longtemps qu'en 2013. (D20-S28)

68% des internautes envisagent un achat sur internet d'ici la fin de l'année. (D20-S28)

La valeur économique pillée par la cybercriminalité en 2013 représente 190 milliards d'euros. (D18-S26)
Pour illustrer un coût :
« Sony s'est fait voler 1,5 million de données de cartes bleues. Le dommage direct : 150 millions. Mais Sony réclame à son assureur 1,3 milliard de dollars pour compenser l'arrêt complet de leur serveur pollué de e-commerce, c'est-à-dire de leurs ventes, la modification de leur système d'information et la campagne de communication qui a suivi. »

Après avoir analysé les données de plus de 100.000 incidents de sécurité sur 10 ans, Verizon a indiqué que 92 % des attaques peuvent être réparties en 9 types de menaces (les attaques de malwares, la perte ou le vol d'appareils, les attaques DDoS, les arnaques à la carte bancaire, les attaques

d’applications web, le cyber-espionnage, les intrusions, le vol interne et les erreurs humaines), ce qui signifie que les entreprises font toujours face aux mêmes risques et aux mêmes attaques, depuis tout ce temps, et à plusieurs reprises. (D12-S19)

Les fraudes en ligne par carte bancaire ont représenté 64,6% du total des fraudes en 2013, soit un rapport de un à vingt par rapport aux magasins physiques. (D11-S18)

Les e-commerçants ne sont que 43 % à utiliser ces méthodes de protection renforcés (par SMS ou par biométrie) 10 millions de français, 33% des Internautes majeurs victimes de cybercrime (Symantec/Norton 2013). (D1-S1)

47% des logiciels étaient piratés en 2005 contre 37% en 2011. (D6-S11)

Les condamnations d’entreprises ayant piraté des logiciels se sont élevées à 1,3 millions d’euros en 2013, en hausse de 30% par rapport à 2012, représentant 12% du montant des condamnations européennes. (D6-S11)

En juin 2014, 3,2 millions de premiers avertissements ont été expédiés depuis sa création et 333.723 deuxièmes avertissements (lettre recommandée) et 71 dossiers transmis à la justice. (D10-S17)

75 % des messages partent de machines classiques (ordinateurs de bureau ou portables, smartphones, tablettes), le reste provient d’appareils connectés. (D3-S6)

Dans 33% des cas, l’introduction d’un malware est réalisée au travers d’une application mobile. (D2-S5)

58% des entreprises pointent l’inefficacité des antivirus du marché pour lutter contre les malwares. (D2-S5)

56% des PC sont infectés via des emails de type « phishing ». (D2-S5)

40% des infections par Malware sont dues aux sites pornographiques. (D2-S5)

Plus de 30% de nos ordinateurs personnels stockent des fichiers illicites à notre insu. (D2-S4).

61% des sites malveillants sont en fait des sites institutionnels. (D1-S1) (D1-S3)

1 site Internet sur 500 est infecté par de malwares (D1-S3)

Google bloque 10000 sites Internet par jour (D1-S3)

400 Millions de personnes sont concernées par des cyberattaques chaque année (D1-S3)

93 % des grandes entreprises ont été victimes d'une cyberattaque en 2012 (D1-S2)

Attaques cybercriminelles +42% en 2012. (D1-S1)

Attaques en ligne +30% en 2012. (D1-S1)

Maliciels sur mobiles +58% en 2012. (D1-S1)

31% des cibles sont des PME en 2012 contre 18% en 2011. (D1-S1)

---

**Denis JACOPINI est à l'origine de cette collecte d'information. Merci de le citer si vous utilisez le résultat de ce travail.**

**Denis JACOPINI est Expert Informatique assermenté et formateur spécialisé en mise en conformité avec la CNIL, en sécurité Informatique, en cybercriminalité et en protection des données à caractère personnel.**

Posez vos questions

---

## MESSAGERIE ÉLECTRONIQUE

144 milliards d’emails sont échangés chaque jour. (D9-S16)

68,8% d’entre eux sont des spams. (D9-S16)

---

**Denis JACOPINI est à l’origine de cette collecte d’information. Merci de le citer si vous utilisez le résultat de ce travail.**

**Denis JACOPINI est Expert Informatique assermenté et formateur spécialisé en mise en conformité avec la CNIL, en sécurité Informatique, en cybercriminalité et en protection des données à caractère personnel.**

Posez vos questions

---

## LES VOLS

3 français sur 10 disent avoir déjà perdu ou s’être fait voler leur téléphone. (D7-S14)

630 000 vols de téléphones portables en 2011. (D5-S9)

160 000 vols de téléphones portables en 2010. (D5-S8)

---

**Denis JACOPINI est à l'origine de cette collecte d'information. Merci de le citer si vous utilisez le résultat de ce travail.**

**Denis JACOPINI est Expert Informatique assermenté et formateur spécialisé en mise en conformité avec la CNIL, en sécurité Informatique, en cybercriminalité et en protection des données à caractère personnel.**

Posez vos questions

---

## RÉSEAUX SOCIAUX

18 % des sociétés de plus de 10 salariés ont un compte dans un réseau social. (D6-S13)

Moins de 13% des sociétés dans le domaine de la construction, du transport ou de l'industrie ont un compte dans un réseau social. (D6-S13)

38 % des sociétés dans le domaine de l'hébergement et de la restauration ont un compte dans un réseau social. (D6-S13)

60 % des sociétés dans le domaine de la communication, de

l’information ou de la réparation d’ordinateurs ont un compte dans un réseau social. (D6-S13)

80% d’entres utilisent les réseaux sociaux pour développer leur image ou commercialiser leurs produits. (D6-S13)

43 % des sociétés de plus de 250 salariés ont un compte. (D6-S13)

5% utilisent les blogs et les sites Internet de partage de contenu multimédia. (D6-S13)

4% utilisent des outils de partage de connaissance. (D6-S13)

Twitter a 900 millions de comptes crées dans le monde mais seulement 241 millions sont actifs. (D5-S11)

Facebook : 1,23 milliard d’utilisateurs actifs dans le monde. (D5-S11)

LinkedIn : 150 millions d’utilisateurs actifs dans le monde. (D5-S11)

Google+ : 300 millions d’utilisateurs actifs dans le monde. (D5-S11)

Tumblr : 166 millions d’utilisateurs actifs dans le monde. (D5-S11)

Viadeo : 55 millions de membres dans le monde dont 8 millions en France et 4,4 millions de visiteurs uniques. (D5-S11)

Instagram : 200 millions d’utilisateurs actifs dans le monde. (D5-S11)

Pinterest : 20 millions d’utilisateurs actifs dans le monde. (D5-S11)

**Denis JACOPINI est à l'origine de cette collecte d'information. Merci de le citer si vous utilisez le résultat de ce travail.**

**Denis JACOPINI est Expert Informatique assermenté et formateur spécialisé en mise en conformité avec la CNIL, en sécurité Informatique, en cybercriminalité et en protection des données à caractère personnel.**

Posez vos questions

---

## ÉQUIPEMENTS DES FRANCAIS

Un foyer sur cinq (21,523%) en France dispose d'une tablette tactile. (D5-S11)

Ils n'étaient que 14,1% au 4e trimestre 2012. (D5-S11)

L'accès à l'Internet mobile double chaque année. (D9-S16)

70% des internautes sont des utilisateurs quotidiens. (D9-S16)

8 nouveaux utilisateurs chaque seconde. (D9-S16)

---

**Denis JACOPINI est à l'origine de cette collecte d'information. Merci de le citer si vous utilisez le résultat**

**de ce travail.**

**Denis JACOPINI est Expert Informatique assermenté et formateur spécialisé en mise en conformité avec la CNIL, en sécurité Informatique, en cybercriminalité et en protection des données à caractère personnel.**

Posez vos questions

---

## LES BLOGS et BLOGUEURS

En France, seulement 4% des blogueurs sont des professionnels. (D4-S7)

65% des blogueurs gagnent 0€ / mois (passion). (D4-S7)

18% des blogueurs gagnent moins de 100€/ mois. (D4-S7)

10% des blogueurs gagnent entre 100€ et 1000€/ mois. (D4-S7)

7% des blogueurs gagnent plus de 1000€/ mois. (D4-S7)

---

**Denis JACOPINI est à l'origine de cette collecte d'information. Merci de le citer si vous utilisez le résultat de ce travail.**

**Denis JACOPINI est Expert Informatique assermenté et formateur spécialisé en mise en conformité avec la CNIL, en sécurité**

**Informatique, en cybercriminalité et en protection des données à caractère personnel.**

Posez vos questions

---

## GOOGLE ET LA PRESSE

Rappelez-vous, en février 2013, Google acceptait de verser 60 millions d'euros à la presse française sur 3 ans. (D8-S15)

Pour l'année 2013, 16 millions d'euros ont été versés. Voici comment ont été dépensés les millions pour les 12 principaux bénéficiaires (23 au total) :
Le Nouvel Observateur a reçu 2 millions d'euro pour créer une édition numérique quotidienne.
L'Express, 1,97 millions pour analyser les données utilisateurs.
Le Figaro, 1,8 millions pour renforcer son site de vidéos.
Le Monde, 1,8 millions pour une future édition du matin sur mobiles.
Ouest-France, 1,4 millions pour deux éditions en ligne par jour.
La Voix du Nord, 840.000 euros pour créer 1524 portails.
La Croix, 835.000 euros pour analyser son audience.
Slate, 758.000 euros pour analyser les conversations numériques

**Denis JACOPINI est à l'origine de cette collecte d'information. Merci de le citer si vous utilisez le résultat de ce travail.**

**Denis JACOPINI est Expert Informatique assermenté et formateur spécialisé en mise en conformité avec la CNIL, en sécurité Informatique, en cybercriminalité et en protection des données à caractère personnel.**

Posez vos questions

---

**Date de la Mises à jour de ce document :** (1) 14/03/2014 – (2) 27/03/2014 – (3) 07/04/2014 – (4) 20/04/2014 – (5) 23/04/2014 – (6) 25/04/2014 – (7) 08/05/2014 – (8) 17/05/2014 – (9) 23/06/2014 – (10) 12/07/2014 – (11) 17/07/2014 – (12) 22/07/2014 – (13) 02/09/2014 – (14) 03/09/2014 – (15) 10/09/2014 – (16) 28/10/2014 – (17) 30/10/2014 – (18) 31/10/2014 – (19) 03/11/2014 – (20) 29/11/2014 – (21) 11/12/20214 – (22) 12/12/2014 – (23) 28/12/2014 – (24) 25/01/2015 – (25) 29/01/2015 – (26) 13/02/2015 – (27) 25/05/2015 – (28) 17/07/2015

**Sources :**
(1)
http://www.symantec.com/fr/fr/about/news/release/article.jsp?prid=20130416_01 (2)
http://www.lemondeinformatique.fr/actualites/lire-%20cybersecurite-en-europe-les-geants-de-l-internet-%20dispenses-de-declarer-les-incidents-56868.html
(3)

https://www.symantec-wss.com/fr/cybercrime4/int/thanks#.Uyr10rK9KSP
(4) Jean-Paul PINTE le 21/03/2014 cours de Cybercriminalité UM1
(5) http://www.testsdintrusion.com/40-infections-malware-dues-aux-sites-pornographiques/
(6) http://www.tomshardware.fr/articles/internet-objet-frigo-spam,1-46695.html
(7) La Quotidienne du 14 04 2014 (France 5) source NWE
(8) http://www.sfr.fr/securite/protection-virus/protection-donnees
(9) http://www.economiematin.fr/les-experts/item/9596-kill-switch-protection-vol-telephone-legislation
(10) http://www.alexitauzin.com/2013/04/combien-dutilisateurs-de-facebook.html
(11) http://www.economiematin.fr/ecoquick/item/7764-etude-equipements-francais-smartphones-tablettes
(12) http://www.zdnet.fr/actualites/logiciels-pirates-13-million-d-euros-de-couts-pour-les-entreprises-francaises-poursuivies-39800283.htm
(13) http://www.zdnet.fr/actualites/les-entreprises-francaises-desertent-les-reseaux-sociaux-selon-l-insee-39800331.htm
(14) http://www.monreseau-it.fr/dossiers/les-antivirus-pour-smartphones-sontils-necessaires-6.htm
(15) http://ecrans.liberation.fr/ecrans/2014/05/15/le-fonds-google-a-verse-16-millions-d-euros-aux-medias-francais-en-2013_1018165
(16) http://www.blogdumoderateur.com/chiffres-internet/
(17) http://www.zdnet.fr/actualites/hadopi-la-machine-a-avertissements-bat-des-records-39803735.htm
(18) http://www.01net.com/editorial/623890/cartes-bancaires-20-fois-plus-de-fraudes-sur-internet-qu-en-magasin/#?xtor=EPR-1-[NL-01net-Actus]-20140716

(19) http://www.huffingtonpost.fr/cyrille-badeau/lutte-cybercriminalite-perdue_b_5595494.html?utm_hp_ref=france
(20) http://www.lepoint.fr/chroniqueurs-du-point/laurence-neuer/google-aux-commandes-du-droit-a-l-oubli-02-06-2014-1830043_56.php
(21) http://www.zdnet.fr/actualites/reprise-d-activite-73-des-entreprises-ne-sont-pas-pretes-apres-un-sinistre-dans-le-cloud-39805553.htm
(22) http://pro.clubic.com/it-business/securite-et-donnees/actualite-725971-etude-15-smartphones-infectes-malware.html
(23) http://www.lemagit.fr/actualites/2240233481/Securite-des-entreprises-francaises-moins-matures-quelles-ne-le-pensent?asrc=EM_MDN_35775718
(24) http://www.zdnet.fr/actualites/byod-des-couts-lies-a-la-securite-parfois-eleves-39808695.htm
(25) https://www.symantec-wss.com/campaigns/15354/fr/assets/infographic/index.html#.VFINvCKG8t4
(26) http://www.paristechreview.com/2014/10/27/espionnage-industriel/
(27) http://www.internetlivestats.com/internet-users/
(28) http://www.commentcamarche.net/news/5865731-les-e-commercants-cibles-par-les-attaques-des-cybercriminels
(29) http://epp.eurostat.ec.europa.eu/cache/ITY_PUBLIC/4-09122014-AP/FR/4-09122014-AP-FR.PDF
(30) http://www.info.expoprotection.com/site/FR/L_actu_des_risques_malveillance__feu/Zoom_article,I1602,Zoom-ce92e8de85306f8f94bb572e6ec6d325.htm
(31) http://www.zdnet.fr/actualites/telechargement-un-avertissement-d-hadopi-ca-calme-39803911.htm
(32) http://pro.clubic.com/e-commerce/paiement-en-ligne/actualite-751153-nfc.html
(33) http://www.globalsecuritymag.fr/Kaspersky-Lab-et-B2B-International,20150128,50328.html
(34) http://www.globalsecuritymag.fr/Le-groupe-Capgemini-lance-une,20150212,50774.html
(35) http://www.info-afrique.com/5336-en-afrique-communication-digitale/

(36) http://www.lesechos.fr/idees-debats/cercle/cercle-135717-comment-les-entreprises-doivent-elles-se-premunir-des-nouvelles-cyberattaques-1137238.php

**Utilisation des repères :** Un repère (D2-S3) indiquera qu'il fait référence à la (D)ate de mise à jour n°2 et à la (S)ource n°3 soit dans notre document, une mise à jour de notre document le 27/03/2014 et la référence https://www.symantec-wss.com/fr/cybercrime4/int/thanks#.Uyr10rK9KSP

**Cet article vous à plu ? Laissez-nous un commentaire (notre source d'encouragements et de progrès)**

---

# La contradiction est manifeste entre la perception des salariés et la réalité en matière de cybersécurité | Le Net Expert Informatique

**Les salariés français ont une connaissance relativement précise des notions liées à la cybersécurité des entreprises. Même si les cyberattaques semblent relativement fréquentes, ils jugent leur entreprise relativement bien protégée sur ces enjeux même si tous ne connaissent pas en détail sa politique en matière de sécurité. Dans ce cadre, ils identifient comme principales menaces : les virus informatiques, le vol de données et la perte de données liée à une erreur humaine. Tels sont les principaux constats que l'on peut tirer de la première étude* portant sur la cybersécurité vue par les collaborateurs, dévoilée ce 17 juin au Bourget par Capgemini et Sogeti.**

Selon l'étude « Cybersécurité, Objets connectés et Systèmes industriels », les salariés français ont dans leur ensemble une connaissance assez précise des différentes notions liées à la cybersécurité : plus des trois quart estiment savoir précisément ce qu'est un virus informatique (88%), un hackeur (80%), un pare-feu (75%) ou une cyberattaque (75%). Seuls les salariés « seniors » sont plus hésitants, même si une majorité d'entre eux reste familier avec ces termes.
Dans ce cadre, 85% des salariés estiment que leur entreprise est bien protégée contre les attaques informatiques et les hackeurs. C'est plus particulièrement le cas des salariés des grandes entreprises pour lesquels ce score monte à 90% (contre 75% pour les PME). Ils jugent ainsi dans leur grande majorité la politique de sécurité informatique de leur entreprise adaptée à leur secteur (85%), efficace (85%) et claire (72%). Elle mériterait toutefois d'être davantage connue (61%).
36% des salariés déclarent que leur entreprise a déjà fait l'objet d'une cyberattaque. Ce score monte à 47% pour les salariés des grandes entreprise. Or, selon Kaspersky, plus de 90% des entreprises ont déjà subi une attaque informatique. Plus spécifiquement, 19% des salariés ont connu une attaque informatique de leur ordinateur professionnel. Pour 5% cela est même régulier. On remarquera que les salariés des PME sont plus nombreux a avoir subi ce type d'attaque que ceux des grandes entreprises. En revanche seule une minorité s'est déjà fait voler du matériel informatique professionnel : 8% un ordinateur, 6% leur téléphone portable. « Ces chiffres contradictoires montrent la complexité de la cybersécurité : celle-ci représente un risque asymétrique pour l'entreprise. Tous les chiffres indiquent que le nombre d'attaques croit considérablement d'année en année (120% de 2013 à 2014) ; attaques dont les salariés de l'entreprise n'ont pas nécessairement connaissance », commente Bernard Barbier, Responsable de la Sécurité des Systèmes d'Information du groupe Capgemini.
Cette contradiction entre la perception des salariés et la réalité de la menace est également illustrée dans le sondage par un fort sentiment de sécurité parmi les salariés. 65% d'entre eux estiment en effet que leur entreprise est plutôt bien protégée, et 20% très bien protégée contre les attaques informatiques et les hackeurs. Ce sentiment est surtout partagé au sein des ETI4 (93%) et des grandes entreprises (90%). « Ce sentiment de sécurité des salariés (65%) est une fois encore en totale contradiction avec les résultats de récentes études démontrant que les campagnes de phishing sont d'une très grande efficacité et qu'elles représentent plus de 80% des attaques réussies. En réalité, il suffit d'un seul PC infecté pour entraîner de lourdes conséquences financières et de réputation pour l'entreprise. On peut par ailleurs se demander si ce sentiment de sécurité n'entraîne pas un manque de vigilance des salariés dans le traitement des messages électroniques venant de l'extérieur de l'entreprise », explique Bernard Barbier.

Au final, les salariés ont trois grandes craintes quand à la cybersécurité de leur entreprise : les virus informatique (pour 48%), le vol de données (43%) et la perte de données suite à une erreur humaine (38%). On notera que les craintes sont fortement liées au secteur d'activité de l'entreprise. Ainsi les salariés de l'industrie craignent davantage le vol de données tandis que ceux du commerce ou du BTP pointent davantage les virus informatiques.

Le vol des données informatiques constitue le premier motif de crainte des salariés. Pour 23% d'entre eux, cela constitue même la plus grosse menace informatique qui pèse sur leur entreprise. De plus, 10% des salariés déclarent avoir subi un vol de leur ordinateur professionnel. « Ces chiffres démontrent la nécessité de protéger les données qui sont au cœur de l'activité de l'entreprise. La priorité est par conséquent de mettre en place des politiques de chiffrement des données : chiffrement des emails et des PC portables », poursuit Bernard Barbier.

Et de préciser que « ce sondage souligne que les salariés de l'entreprise ont un sentiment positif quant à la sécurité de leur système d'information classique. En revanche, la perception du niveau de sécurité des systèmes industriels (contrôle commande des usines) semble avoir plusieurs années de retard car la cyber menace est plus récente. Pourtant, le danger est plus dramatique encore, avec des conséquences matérielles et humaines, comme dans l'hypothèse d'une explosion d'usine. Le cyber terrorisme pourrait d'ailleurs viser en priorité ce domaine dans un avenir proche ».

Didier Appell, responsable, au sein de l'entité sectorielle mondiale « Cybersecurité » du Groupe, de l'offre Cybersécurité industrielle de Sogeti High Tech, le pôle d'expertise en Ingénierie et conseil en technologies du groupe Capgemini, précise : « Les entreprises ont fourni de gros efforts pour sensibiliser leurs salariés aux risques que représentent les attaques cybernétiques. Par extension, cette sensibilisation doit être également portée sur les systèmes industriels de supervision, de commande et contrôle ainsi que des systèmes embarqués car là aussi nous relevons une contradiction entre la perception des salariés et la réalité des menaces. Nous sommes effectivement de plus en plus sollicités par nos clients pour les aider à renforcer leur sécurité sur tous ces aspects ».

* L'étude a été réalisée auprès d'un échantillon de 1010 salariés français de bureau d'entreprises privées. La représentativité de l'échantillon est assurée selon la méthode des quotas sur les critères de sexe, d'âge, de catégorie socioprofessionnelle, de taille d'entreprise, de secteur d'activité de l'entreprise, de statut de l'employeur (public/privé) et de région de résidence. L'échantillon a été interrogé en ligne sur système CAWI (Computer Assistance for Web Interview) du 13 au 26 mai 2015.

---



---



---



Source : http://www.infodsi.com/articles/156643/contradiction-est-manifeste-entre-perception-salaries-realite-matiere-cybersecurite.html

---

# Les cyber-attaques changent de forme…| Le Net Expert Informatique

## Les cyber-attaques changent de forme…

**Akamai constate une évolution du profil des attaques informatiques par déni de service distribué (DDoS), mais aussi des assauts contre les services Web.**

Le profil des attaques informatiques par déni de service distribué (DDoS, visant à rendre des ressources indisponibles en les saturant de requêtes) a fortement évolué en un an, tandis que de nouvelles menaces sont nées de l'adoption du protocole IPv6.
Telles sont les principales conclusions émises par Akamai dans la dernière édition de son baromètre Internet Security – document PDF, 93 pages – portant sur le 1er trimestre 2015.
Sur le volet DDoS, le constat est sans appel : les assauts se multiplient (+ 116,5 % d'une année sur l'autre). Les attaques sur la couche applicative (Layer 7) augmentent de 60 %, mais ne représentent encore qu'un cas sur dix.
Le reste des offensives se concentre sur l'infrastructure (Layers 3 & 4 ; + 125 %), qui permet de maximiser plus facilement la puissance des attaques tout en nécessitant moins de ressources.
Alors qu'un DDoS s'échelonnait en moyenne sur 17 heures au 1er trimestre 2014, la durée a avoisiné les 25 heures un an plus tard (+ 43 %). Des attaques plus longues, donc, mais aussi moins virulentes : 5,95 Gbit/s de bande passante moyenne, contre 9,7 Gbit/s un an plus tôt ; quant au nombre moyen de paquets envoyés par seconde, il baisse de 89 % (2,21 millions).
Akamai a tout de même relevé 8 attaques d'un volume supérieur à 100 Gbit/s.
Encore quasiment inexploité début 2014, le SSDP (« Simple Service Discovery Protocol ») est devenu, en l'espace d'un an, le principal facteur déclencheur des attaques DDoS (plus d'un cas sur cinq). Implémenté et activé par défaut sur des millions d'équipements (routeurs, webcams, imprimantes, TV connectées) pour leur permettre d'interagir sur un réseau local, ce protocole est souvent mal – ou pas du tout – sécurisé.
L'industrie du jeu vidéo concentre à elle seule 35 % des dénis de services répertoriés entre le 1er janvier et le 31 mars. Suivent le secteur IT (25 %), les télécoms (14 %), la finance (8,4 %), les médias (7,5 %), l'éducation (5 %), la distribution (2,3 %) et le secteur public (2 %).
Pour la première fois, Akamai inclut dans son baromètre les attaques contre les applications Web. Les analyses réalisées sur environ 180 millions d'échantillons ont permis de dégager 7 vecteurs de piratage.
Dans les deux tiers des cas, les cybercriminels ont exploité une faille de type LFI (« Local File Inclusion ») leur permettant d'accéder, en lecture, à des fichiers hébergés sur un serveur Web. On notera cette campagne massive venue d'Allemagne contre deux grands noms du secteur de la distribution via une vulnérabilité dans le plugin WordPress RevSlider.

**SQL, HTTPS et IPv6**
29 % des attaques recensées sont liées à des injections SQL* ; c'est-à-dire à l'exploitation d'une brèche dans une application qui interagit avec une base de données en introduisant une requête SQL non prévue par le système. Illustration avec cette campagne issue essentiellement d'Irlande et visant une société de l'industrie du voyage.
Les autres types d'attaques (inclusion de fichiers distants sur des serveurs Web, injection de code PHP, exécution de commandes shell sur le système visé…) n'ont été repérées que dans environ 5 % des cas. Sachant toutefois qu'au global, près de 10 % ont été menées sur des sites « sécurisés » en HTTPS…
Parmi les grandes tendances de l'année, Akamai pointe la menace grandissante des sites dits « booters » ou « stressers » et qui permettent de simuler des attaques DDoS. Alors qu'il y a encore un an, leur ampleur se limitait à 10 ou 20 Gbit/s, ils peuvent désormais lancer des assauts dévastateurs à plus de 100 Gbit/s, en exploitant notamment des techniques de réflexion du trafic.
Autre enjeu à surveiller : l'adoption du protocole IPv6, qui permet d'élargir l'espace d'adressage réseau… mais dont l'architecture est dite « imparfaite » par Akamai : il est possible de passer outre certaines protections implémentées dans IPv4. Il existe d'ailleurs « plusieurs signes » montrant que les cybercriminels mènent bien des recherches sur le sujet.
* Documentées depuis 1998, les attaques par injection SQL vont désormais bien au-delà du simple vol de données. Elles permettent aussi l'élévation de privilèges, l'exécution de commande, la corruption de systèmes…

---



---



---



Source : http://www.itespresso.fr/securite-it-cyber-attaques-changent-forme-97172.html

# Les dernières fuites de données mettent en évidence la nécessité de sécuriser les e-mails | Le Net Expert Informatique

| | |
|---|---|
| | Les dernières fuites de données mettent en évidence la nécessité de sécuriser les e-mails |

**Peut-on se passer de l'e mail dans le cadre de ses activités professionnelles ? Pratique et instantanée, la communication par e-mail s'est imposée au quotidien dans l'entreprise. Certaines études évaluent à plus de 100 milliards le nombre d'e-mails professionnels qui sont échangés chaque jour(1).**

**Nos e mails risquent-ils de laisser échapper des données sécurisées ?**
Malgré ses nombreux atouts, l'e-mail présente également certains risques. Des récits de fuites de données sensibles font régulièrement la une des médias. Un des derniers incidents en date : la récente divulgation des numéros de passeport de 31 leaders mondiaux. En cause ? La fonctionnalité de saisie automatique à partir du carnet d'adresses d'Outlook. Cette fonctionnalité – aussi pratique soit-elle – ne fait qu'accentuer le risque de diffuser, par erreur, des données confidentielles.
Malgré l'augmentation du nombre d'erreurs d'aiguillage d'e-mails et l'évolution du contexte législatif – comme en atteste la récente loi australienne sur l'obligation de conserver des métadonnées et d'autres textes réglementant la transmission de données confidentielles (HIPAA, FIPPA et PCI) –, on peut s'étonner que les entreprises ne soient pas plus nombreuses à choisir de sécuriser le contenu de leurs e mails.
L'e mail est sans doute un peu trop pratique à en juger par la facilité avec laquelle des informations sensibles peuvent être envoyées, au risque de tomber dans les mauvaises mains.

**Quelques chiffres :**
• 53 % des employés ont déjà reçu des données sensibles d'entreprise non cryptées par e mail ou en pièces jointes (2).
• 21 % des employés déclarent envoyer des données sensibles sans les chiffrer(2). Les coûts liés à la perte de données s'envolent, sans parler des conséquences sur la réputation des entreprises et des éventuelles répercussions sur le plan juridique en cas de violation de la réglementation sur la transmission et le stockage de données confidentielles (notamment dans le cadre des lois HIPAA et FIPPA, et du standard PCI).
• 22 % des entreprises sont concernées chaque année par la perte de données via e-mail(3).
• 3,5 millions de dollars : coût moyen d'une violation de données pour une entreprise(4).

**La solution**
Il existe heureusement des solutions de sécurité des e-mails qui mettent les utilisateurs et leur entreprise à l'abri de ces menaces. La signature numérique et le chiffrement des e-mails garantissent la confidentialité d'un message et évitent que des données sensibles ne tombent dans de mauvaises mains. Le destinataire a également l'assurance de l'identité réelle de l'expéditeur de l'e-mail et que le contenu du message n'a pas été modifié après son envoi.
Le chiffrement d'un e-mail revient à sceller son message puis à le déposer dans un dossier verrouillé dont seul le destinataire prévu possède la clé. Il est alors impossible pour une personne interceptant le message, pendant son transit ou à son emplacement de stockage sur le serveur, d'en voir le contenu. Sur le plan de la sécurité, le chiffrement des e mails présente les avantages suivants :
• Confidentialité : le processus de chiffrement requiert des informations de la part du destinataire prévu, qui est le seul à pouvoir consulter le contenu déchiffré.
• Intégrité du message : une partie du processus de déchiffrement consiste à vérifier que le contenu du message d'origine chiffré correspond au nouvel e-mail déchiffré. Le moindre changement apporté au message d'origine ferait échouer le processus de déchiffrement.
Avant de choisir une solution, il est important d'avoir en tête plusieurs choses. L'utilisateur est le mieux placé, car il connaît son entreprise mieux que personne. Phishing, perte de données… quels sont ses principaux sujets de préoccupation ? Quelle est l'infrastructure de messagerie en place dans l'entreprise ? Quel est le cadre réglementaire ? Les réponses propres à chaque entreprise orienteront les choix vers la solution la plus appropriée.

Sources :
(1) Email Statistics Report 2013-2017, The Radicati Group, Inc.
(2) SilverSky Email Security Habits Survey Report, SilverSky, 2013
(3) Best Practices in Email, Web, and Social Media Security, Osterman Research, Inc., January 2014
(4) Global Cost of Data Breach St'sudy, Ponemon Institute,

---



---



---



Source : http://www.globalsecuritymag.fr/Les-dernieres-fuites-de-donnees,20150601,53078.html
par GlobalSign