Résultats exclusifs :
rapport de l'enquête sur les risques informatiques mondiaux 2014

Menaces et atteintes à la sécurité informatique

Impression versus réalité : il est temps de réajuster

Table des matières

À propos du rapport sur les risques informatiques mondiaux

Publié pour la quatrième année consécutive, le **rapport annuel de Kaspersky Lab sur les risques informatiques mondiaux** recueille des informations stratégiques obtenues auprès de professionnels de l'informatique du monde entier. Fruit d'une enquête réalisée par les experts du cabinet d'études de marché "B2B International", dont les résultats ont été analysés l'équipe d'experts en cyber-sécurité de Kaspersky Lab, ce rapport fournit un éclairage pertinent sur les attitudes et stratégies prédominantes chez les professionnels vis-à-vis de la sécurité informatique. Il sert aussi de comparatif du secteur pour aider les entreprises à comprendre le type et la dangerosité des menaces informatiques qui pèsent sur leurs activités.

Pourquoi lire ce rapport ?

- Il fournit des conclusions globales et par thématique
- Il apporte un éclairage exclusif sur les points de vue et stratégies des professionnels de l'informatique dans le monde entier
- Il vous aide à comparer les mesures informatiques mises en place au sein de votre entreprise à celles de vos homologues du secteur

Rapport sur les risques informatiques mondiaux 2014 :

Résumé analytique

L'enquête en quelques mots :

- **3 900 entreprises interrogées**
- **27 pays**
- **Période couverte : avril 2013 - mai 2014**
- **Personnes interrogées : professionnels de l'informatique ayant de « bonnes connaissances » des problèmes informatiques**

En 2013 et 2014, la sécurité informatique a pris de l'ampleur, passant d'une simple inquiétude à un sujet d'actualité mondial : ces derniers temps, les fuites de données, l'espionnage industriel et la cyber-criminalité ont souvent fait les gros titres. Mais au-delà de l'agitation médiatique, quelle est la réalité de la situation et en quoi vous concerne-t-elle ?

Alors que l'économie mondiale commence à se rétablir, les réflexions stratégiques à long terme reprennent le devant dans les conseils d'administration. L'attention portée à la croissance redevient essentielle et l'on ne se contente plus de survivre jusqu'au prochain exercice financier, ce qui entraîne une évolution des priorités. Les stratégies de gestion du risque reprennent ainsi de l'importance. Mais celles-ci ne sont efficaces que lorsqu'elles s'appuient sur une compréhension approfondie du paysage actuel des menaces.

L'un des points les plus intéressants mis en évidence dans le rapport de cette année est ce que nous avons baptisé « **le décalage d'impression** », c'est-à-dire l'écart existant entre la façon dont les professionnels perçoivent les événements et la réalité sur le terrain.

En 2013 et 2014, Kaspersky Lab a détecté environ 315 000 échantillons malveillants chaque jour. Or, il s'avère que seulement **4 %** des entreprises interrogées connaissent le chiffre exact. Pour détailler, **91 %** d'entre elles le sous-estiment et **70 %** pensent que le nombre de menaces quotidiennes est inférieur à 10 000. Cette erreur d'appréciation est éloquente.

Mais ce n'est pas tout.Si **94 %** des entreprises déclarent avoir subi une menace extérieure, seulement **68 %** ont déployé une protection complète contre les logiciels malveillants sur leurs postes de travail, et seulement **44 %** utilisent des solutions de sécurité pour leurs appareils mobiles.

94 % des entreprises ont subi une menace extérieure

Comment résoudre le problème ? Il faut réajuster nos impressions pour prendre conscience des menaces de façon plus réaliste, ne pas se limiter aux atteintes les plus visibles. Il faut aussi tenir compte des risques quotidiens et permanents.

Le contrôle et l'intégration des appareils mobiles au travail quotidien et la sécurité liée à la virtualisation font partie des principales inquiétudes. Pourtant, seulement **34 %** des décideurs informatiques ont une compréhension claire des solutions de sécurité virtuelle disponibles, et **46 %** des entreprises estiment que leurs solutions de sécurité classiques les protègent suffisamment.

L'impact **estimé** des piratages de données pour les PME a baissé de **12 %**, passant de **54 000** à **48 000 $**, alors que celui pour les grands groupes a augmenté de **14 %**, passant de **700 000** à **798000 $**, mais il s'agit peut-être uniquement d'un ressenti. Les grands groupes sont mieux équipés pour détecter les vulnérabilités, tandis que les PME n'ont pas forcément conscience d'avoir été attaquées.

Cet impact n'est pas aussi simple qu'on peut le croire de prime abord. **87 %** des entreprises ayant subi des pertes de données ont dû faire appel à des services professionnels, et près de la moitié (**47 %**) ont engagé des frais supplémentaires conséquents. L'année dernière, le coût des « dommages types » (services professionnels, périodes d'arrêt forcé et manque à gagner) causés aux PME par un événement grave était évalué à 35 000 $ en moyenne. Chez les grands groupes, ce chiffre atteint 690 000 $.

L'impact des piratages de données sur la confiance et la réputation est aussi très apparent : **82 %** des entreprises se déclarent prêtes à changer d'établissement financier si celui-ci subit un piratage, tandis que **27 %** estiment que les mesures prises par les banques pour protéger leurs informations financières sont insuffisantes.

82 % des entreprises se déclarent prêtes à changer d'établissement financier si celui-ci subit un piratage

Il existe toutefois des dissensions concernant la responsabilité de la protection des informations financières : seulement **35 %** des clients pensent qu'elle incombe aux établissements financiers, tandis que **85 %** de ces derniers se considèrent effectivement responsables.

Que peut-on conclure de ces chiffres ? Les entreprises sont en progrès, mais les cyber-criminels aussi. Malgré l'existence d'outils permettant aux entreprises de se protéger, la plupart d'entre elles continuent d'afficher une attitude passive vis-à-vis de la sécurité informatique. Elles doivent être plus proactives et cesser de sous-estimer la diversité, le nombre et le degré de sophistication des menaces modernes. En clair, les solutions antivirus classiques ne suffisent plus.

Les entreprises doivent prendre conscience de la complexité du problème auquel elles sont confrontées. La mise en place d'une défense à plusieurs niveaux face aux menaces posées par les facteurs « humains », par la prolifération des appareils utilisés et par l'émergence des nouvelles technologies est désormais essentielle, car aucune entreprise ne dispose des ressources humaines suffisantes pour gérer cela toute seule.

Il est temps de procéder à un important réajustement de la façon dont les problèmes de sécurité sont perçus et traités. Les entreprises doivent faire preuve de davantage de proactivité et de vigilance et s'informer, sous peine de se retrouver à la Une de l'actualité de la sécurité informatique.

En clair, les solutions antivirus classiques ne suffisent plus

Rapport sur les risques informatiques mondiaux 2014 :

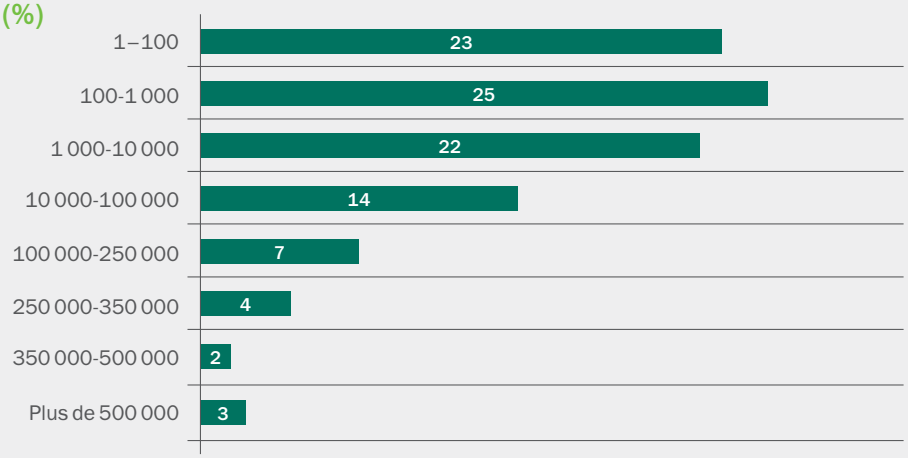
1 Entre impression et réalité : comment réduire l'écart ?

> **L'écart entre l'image du panorama des menaces auprès des entreprises et sa réalité ne cesse de se creuser. Nous avons baptisé ce phénomène « le décalage d'impression ». Il montre que les entreprises de toutes tailles sous-estiment largement tant la quantité que la gravité des menaces qui pèsent sur elles.**
> Costin Raiu, Global Research & Analysis Team, Kaspersky Lab

En tant que décideur informatique, vous assumez la responsabilité des systèmes et de l'infrastructure stratégiques de l'entreprise. Vous les protégez contre les menaces, empêchez les pertes de données et faites en sorte que tout fonctionne de manière optimale. Et en général, vous y parvenez. Mais qu'en est-il de ces moments où vous n'y arrivez pas ? Avez-vous une idée concrète de ce que vous laissez passer ?

Une prise de conscience peut s'avérer nécessaire. Il faut parfois savoir réviser son jugement pour s'adapter à la nature en constante mutation des menaces auxquelles on est confronté. **91 %** des décideurs professionnels sous-estiment le nombre d'échantillons de menaces découverts chaque jour, et seulement **4 %** d'entre eux ont une idée précise du chiffre réel. Pour être plus précis, la majorité d'entre nous sous-estime considérablement ce chiffre, puisque nous sommes **70 %** à penser que moins de 10 000 nouveaux échantillons sont découverts chaque jour. Le chiffre réel d'après les détections de Kaspersky Lab s'élève à 315 000.

Nombre perçu de nouveaux échantillons de échantillons de programmes malveillants découverts chaque jour (%)



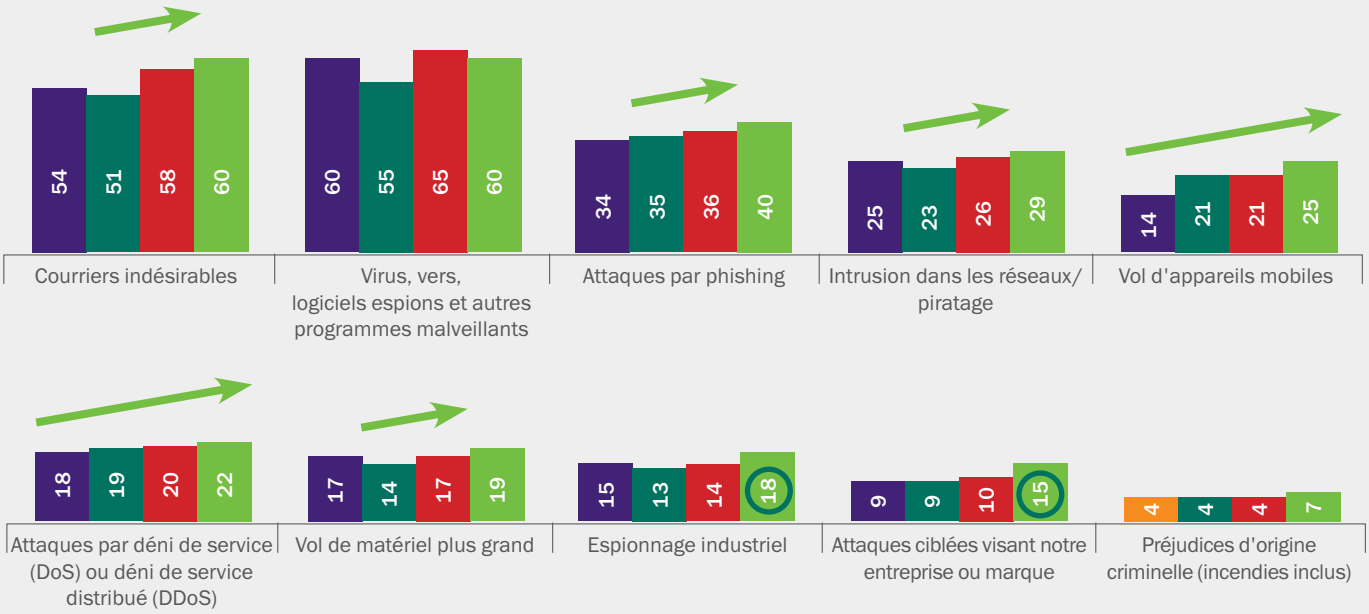
Pourtant, malgré cette sous-évaluation, les personnes interrogées indiquent une hausse de leur impression du nombre de cyber-attaques chaque année aux cours des quatre dernières années. Cela est peut-être dû au fait que la plupart des entreprises pensent que le nombre de menaces les concernant a augmenté, mais n'ont pas d'idée précise de la situation générale.

Des entreprises de toutes tailles citent la hausse du volume de courriers indésirables, de tentatives de phishing et d'attaques DDoS comme source d'inquiétude. L'espionnage industriel et les attaques ciblées progressent également. Le nombre d'entreprises signalant des attaques spécifiques les visant directement a augmenté de **5 %** depuis 2013, pour atteindre aujourd'hui **15 %**.

Que se cache-t-il vraiment derrière toutes ces menaces ?

Menaces externes subies

94 % des entreprises ont subi une menace extérieure. D'autres tendances claires émergent, comme la hausse régulière des attaques de déni de service au cours des quatre dernières années.



Pourcentage d'entreprises subissant chaque événement

2011 (n=1 408) 2012 (n=2 376) 2013 (n=1 912) 2014 (n=2 119)

Hausse significative d'une année sur l'autre

Une idée reçue courante est que les programmes malveillants sont spécifiques et discrets, et non intégrés aux cyber-attaques. Bien que le nombre d'attaques malveillantes signalées ait baissé entre 2013 et 2014, il s'agit toujours de la menace informatique la plus courante et la plus dangereuse. Les attaques de phishing, par DDoS et ciblées utilisent toutes des programmes malveillants de plus en plus sophistiqués.

Et en dépit des mesures mises en œuvre, d'importantes failles subsistent dans les systèmes de sécurité informatique, quelle que soit la taille de l'entreprise.

Malgré la nature de la menace que constituent les programmes malveillants, seulement **68 %** des entreprises déploient des logiciels anti-programmes malveillants sur leurs postes de travail, **42 %** utilisent des solutions de sécurité mobile et **52 %** de toutes les entreprises interrogées installent régulièrement les correctifs et mises à jour pour leurs produits de sécurité, une tâche pourtant essentielle pour empêcher les attaques malveillantes ou le piratage des données.

Au mieux, cela suggère que les entreprises ne sont que partiellement protégées. Au pire, on peut considérer qu'elles sont très mal préparées aux menaces qui pèsent sur elles.

Comment les entreprises peuvent-elles alors réduire l'écart ? En améliorant leur compréhension de la vraie nature de ces menaces et en déployant et tenant effectivement à jour leurs solutions de sécurité.

Rapport sur les risques informatiques mondiaux 2014 :

2 Les menaces complexes nécessitent une protection multi-niveaux

À l'heure actuelle, les entreprises du monde entier font face à des menaces de plus en plus complexes. Et malheureusement, un seul produit ou une seule approche ne suffit plus à les protéger contre les différents types de programmes malveillants ou virus. La politique de la « réponse unique » n'a ni l'envergure, ni la capacité nécessaires pour empêcher différentes attaques contre leur infrastructure informatique.

Pour ne rien arranger, les programmes malveillants évoluent rapidement et changent quotidiennement. L'ennemi avance masqué, et se déplace constamment. Fin 2013, on recensait 200 000 échantillons de codes de programmes malveillants mobiles différents. Six mois plus tard, 175 000 autres venaient grossir ce chiffre. Cette hausse inquiétante doit être prise en compte dans la définition des stratégies de sécurité à appliquer pour protéger les données et transactions financières et maintenir la continuité des services face aux attaques DDoS.

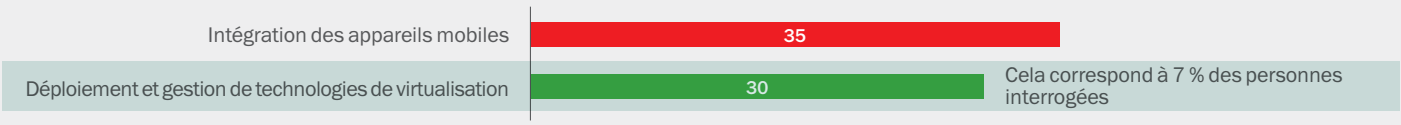
> **L'une des statistiques les plus inquiétantes de l'étude est le très faible taux d'application et de gestion des correctifs. Étant donné que la majorité des atteintes à la sécurité sont liées à une vulnérabilité d'une application non corrigée, cela devrait être l'une des priorités de tout professionnel de l'informatique.**
>
> Sergey Lozhkin, Global Research & Analysis Team, Kaspersky Lab

Il faut rappeler que ce qui convient à une entreprise n'est pas forcément adapté à une autre. Il est essentiel de se doter de la bonne solution pour le réseau de l'entreprise, qu'il s'agisse d'un LAN, de réseaux sans fil ou cellulaires, de WAN ou de communications sur IP, ou encore d'un mélange de ces technologies. Les solutions de sécurité doivent fonctionner de manière efficace sur ces plates-formes sans compromettre la sécurité ou les performances. Et avec la virtualisation qui concerne de plus en plus d'entreprises, ainsi que le rôle croissant des appareils mobiles dans le monde professionnel, il est plus important que jamais que les entreprises prennent conscience du besoin d'une protection multi-niveaux et intégrée, couvrant les appareils physiques, mobiles et virtuels.

Comme l'indique le graphique ci-dessous, parmi les personnes interrogées considérant que la gestion du changement est l'une de leurs priorités, **30 %** déclarent que le déploiement et la gestion de technologies de virtualisation représentent leur principale difficulté, tandis que **35 %** estiment qu'il s'agit davantage de l'intégration des appareils mobiles.

GESTION DU CHANGEMENT DES SYSTÈMES INFORMATIQUES

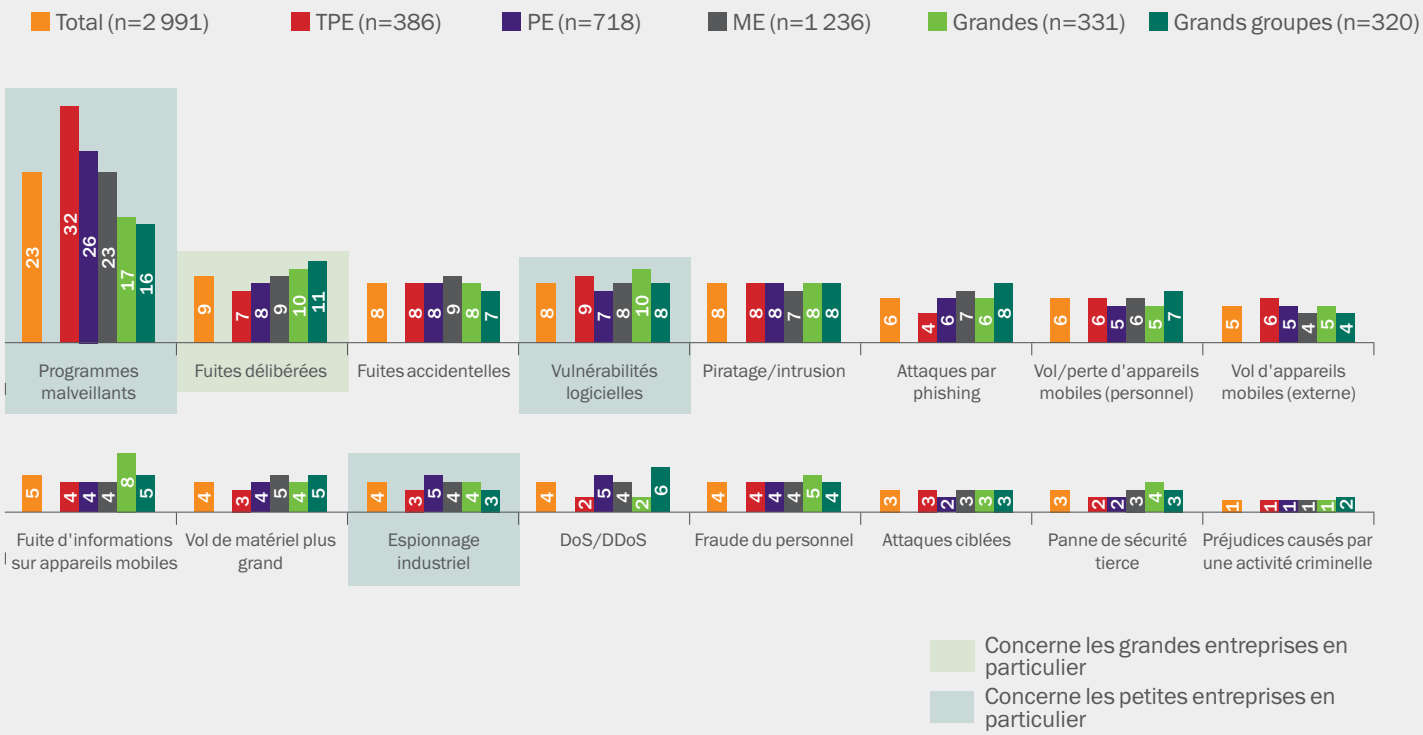
Parmi les 22 % de personnes interrogées considérant que la gestion du changement est une priorité, le mobile et la virtualisation sont les principales difficultés



Le graphique suivant met en évidence les menaces pesant sur les grandes et petites entreprises, des programmes malveillants aux fuites de données, en passant par l'espionnage industriel et le vol des appareils mobiles.

PERTE DE DONNÉES LA PLUS GRAVE

Actuellement, les programmes malveillants sont la première cause de pertes de données graves. Le problème est moins inquiétant au sein des grandes entreprises, davantage préoccupées par les fuites délibérées d'informations.



Base : toutes les personnes interrogées ayant perdu des données, quelle que soit la taille de l'entreprise

D'après le graphique ci-dessus, il est évident que les programmes malveillants sont la principale cause des pertes de données. Mais alors, comment les entreprises ont-elles pu percevoir entre 2013 et 2014 une baisse de **5 %** des attaques malveillantes ? Pour faire simple, **91 %** des entreprises sous-estiment le nombre de nouveaux échantillons découverts chaque jour, et la plupart d'entre elles n'ont pas conscience que la majorité des attaques ciblées telles que le phishing et les DDoS intègrent en leur sein un programme malveillant. Ce n'est pas tant que les infiltrations de programmes malveillants ont baissé, c'est surtout que les attaques ne sont pas forcément perçues comme des attaques de programmes malveillants.

Que peut-on déduire de ces constatations ?

1. Les solutions antivirus classiques ne sont plus efficaces et ne disposent pas de l'étendue et de l'échelle de protection requise par les entreprises.
2. La complexité croissante de l'infrastructure informatique fournit davantage d'opportunités aux attaques malveillantes.
3. Les erreurs humaines et d'appréciation ne peuvent pas être ignorées, et l'explosion du Bring Your Own Device (BYOD) favorise les failles d'exploitation.

Rapport sur les risques informatiques mondiaux 2014 :

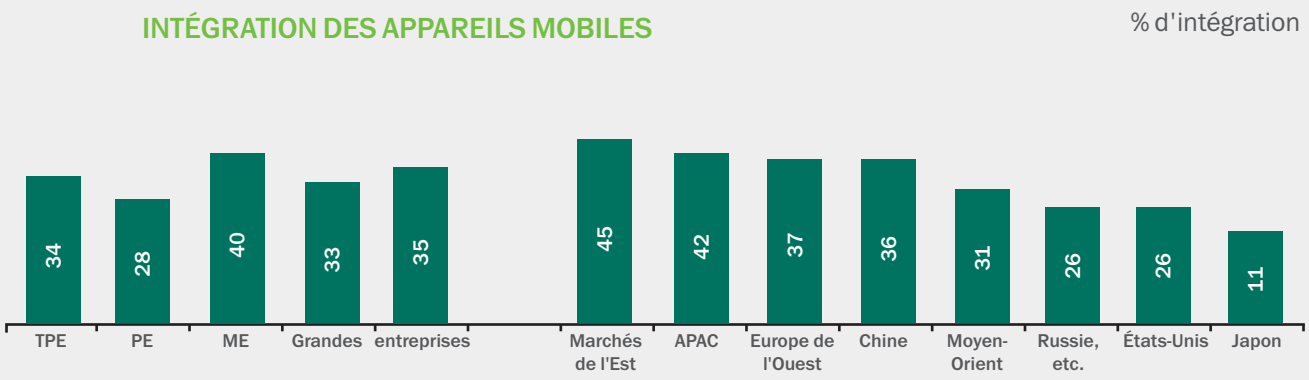
3 La prise de conscience du risque sur mobile

Partout dans le monde, le travail mobile est rapidement adopté par les entreprises. Mais son point fort, à savoir sa capacité à aider les collaborateurs à gagner en flexibilité, ne vaut rien si les mesures de sécurité adéquates ne sont pas mises en place. Un appareil mobile non protégé permet d'atteindre les données sensibles et donne aux cyber-criminels un point d'accès aisé à un système par ailleurs protégé.

C'est la raison pour laquelle **35 %** des entreprises reconnaissent que l'intégration des appareils mobiles est l'une des principales difficultés de l'année à venir. Et le sujet ne concerne pas que les grandes entreprises. L'intégration des appareils mobiles est essentielle pour les entreprises de toutes tailles, comme le montre le graphique ci-dessous. Seules les petites entreprises, avec **28 %** des personnes interrogées, n'érigent pas l'intégration du mobile au rang de priorité. Toutefois, cela est peut-être dû au fait que les petites entreprises sous-estiment les menaces potentielles liées aux appareils mobiles.

24 % des entreprises citent le BYOD parmi les principales priorités de sécurité informatique au cours des 12 prochains mois, et ce chiffre s'élève à 32 % chez les TPE. Cela n'est pas vraiment étonnant étant donné que **42 %** des entreprises réalisent actuellement des transactions sensibles sur mobile.

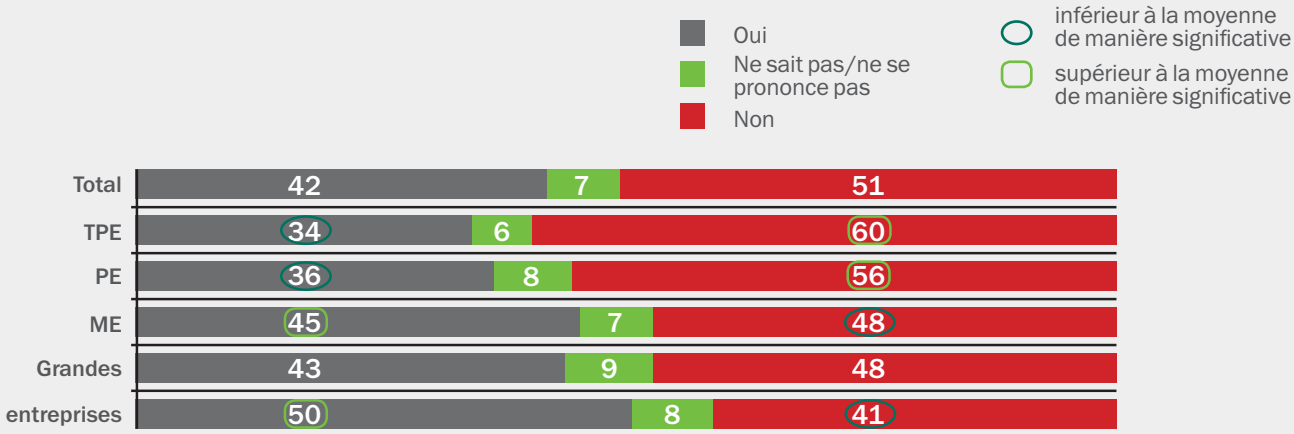
INTÉGRATION DES APPAREILS MOBILES



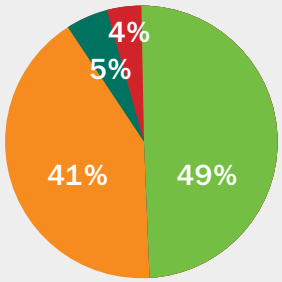
> **Nous savons tous que les entreprises sont plus mobiles, mais le profil d'utilisation évolue. Nous voyons désormais des entreprises qui utilisent des appareils mobiles pour partager des informations sensibles et même conclure des transactions financières.**
>
> David Emm, Kaspersky Lab, Global Research & Analysis Team

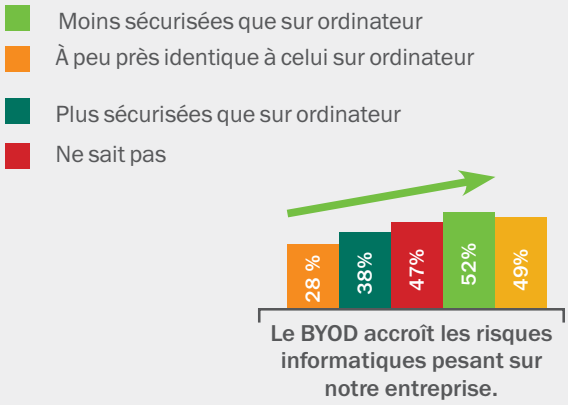
UTILISATION ET ATTITUDES VIS-À-VIS DES TRANSACTIONS MOBILES

Votre entreprise effectue-t-elle des transactions sensibles sur mobile ?



Quel est le degré de sécurité des transactions sur mobile ?





Le BYOD accroît les risques informatiques pesant sur notre entreprise.

Ce qui l'est plus en revanche, c'est que moins de la moitié **(49 %)** d'entre elles considèrent les appareils mobiles comme moins sécurisés que les ordinateurs. **41 %** considèrent que leur appareil mobile est aussi sécurisé que leur ordinateur, **5 %** considèrent que leur appareil mobile est plus sécurisé, et **4 %** ne se prononcent pas.

Il est intéressant de constater que les entreprises de toutes tailles considèrent le BYOD comme une menace pour la sécurité. Cependant, la perception de cette menace change selon le type de structure. Globalement, plus l'entreprise est grande, plus elle s'inquiète des risques de sécurité liés au BYOD. **28 %** des TPE considèrent que cette menace est en hausse, contre **47 %** et **49 %** pour les entreprises de taille moyenne et les grandes entreprises respectivement.

Et elles n'ont pas tort. Au cours des quatre dernières années, **30 %** des entreprises ont subi une perte ou un vol d'appareil mobile. Et bien que la perte de données qui s'en suit ait baissé au cours des deux dernières années, passant de **26 %** en 2012 à **21 %** en 2014, il s'agit toujours de la deuxième cause de perte de données professionnelles, derrière le partage de données accidentel par le personnel.

Au cours des quatre dernières années, 30 % des entreprises ont subi une perte ou un vol d'appareil mobile.

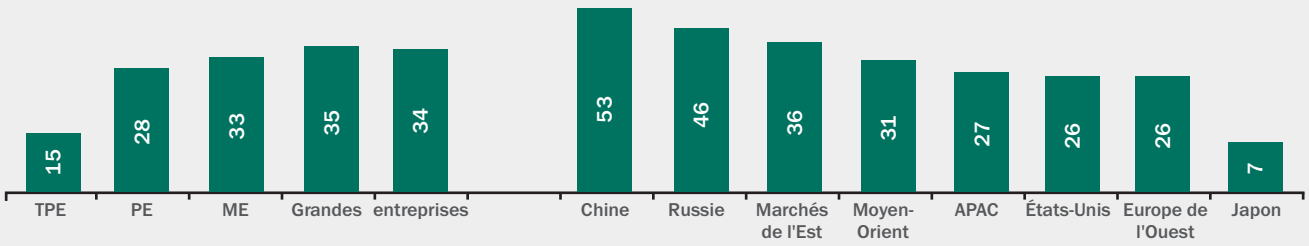
Rapport sur les risques informatiques mondiaux 2014 :

4 Virtualisation : protection des nouveaux environnements de travail

Pour de nombreuses entreprises, la virtualisation est intégrée à la stratégie informatique depuis un certain temps déjà, mais la mise en œuvre concrète de mesures de sécurité spécifiques dans ce domaine est marginale. Ce problème n'est pas ignoré pour autant, puisqu'il a été cité comme une priorité informatique essentielle pour les 12 mois à venir par **14 %** des entreprises interrogées. Le chiffre atteint même **21 %** chez les grands groupes.

DÉPLOIEMENT ET GESTION DE TECHNOLOGIES DE VIRTUALISATION

%, dans chaque catégorie, citant la gestion du changement vers la virtualisation, comme un défi auquel ils sont actuellement confrontés



> **La virtualisation occupe une place de plus en plus importante au sein de la stratégie informatique des entreprises. Mais lorsqu'il s'agit d'adopter des solutions de sécurité spécialisées, la plupart d'entre elles ne comprennent pas clairement les solutions disponibles ou les impératifs de sécurité que crée un environnement virtualisé.**
> Sergey Lozhkin, Global Research & Analysis Team, Kaspersky Lab

La virtualisation inquiète davantage les grandes que les petites entreprises. Plus d'un tiers des entreprises de taille moyenne, grandes entreprises et grands groupes la citent comme un défi à relever, contre **28 %** des petites entreprises et **15 %** des TPE.

La compréhension des options de sécurité pour la virtualisation est variable, même chez les professionnels de l'informatique. Seulement un tiers des entreprises interrogées déclare comprendre clairement les solutions disponibles, et un quart d'entre elles avoue les comprendre peu, voire pas du tout.

GLOSSAIRE :

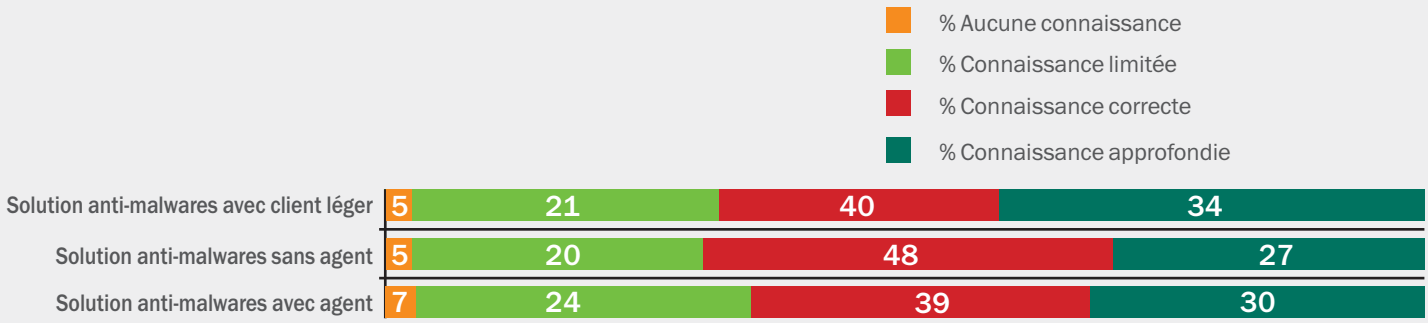
Les trois types de solutions de sécurité pour réseaux virtuels offrent différentes options de sécurité et sont déployés idéalement de différentes façons.

Sans agent : basé sur la technologie Push, conception centralisée. Il est contrôlé par une console centrale et ne nécessite aucune installation d'agent sur les machines, physiques ou virtuelles. Il peut permettre de baisser les coûts, réduire le temps de gestion et se déploie facilement dans les grandes entreprises.

Avec agent : basé sur la technologie Pull, nécessite un logiciel côté client avant de fournir des mises à jour au serveur. Les solutions avec agent sont recommandées pour les utilisateurs itinérants et les machines déconnectées, et peuvent être un complément utile aux solutions sans agent.

Agent léger : fonctionne en redirigeant les charges de travail les plus conséquentes vers une appliance virtuelle tout en protégeant les terminaux contre les menaces. L'agent léger mélange les solutions sans et avec agent.

CONNAISSANCE DES SOLUTIONS DE SÉCURITÉ POUR LES ENVIRONNEMENTS VIRTUELS AU SEIN DE LA COMMUNAUTÉ DES EXPERTS DE LA SÉCURITÉ



24 % des entreprises pensent que leur solution de sécurité actuelle leur fournit une meilleure protection et surtout de meilleures performances que les solutions spécialisées. **20 %** déclarent ne rencontrer aucun problème avec leurs solutions classiques et **13 %** considèrent que la menace pesant sur leur environnement virtualisé ne justifie pas le coût supplémentaire de mise en œuvre d'une solution spécialisée.

En dépit d'une compréhension variable des options de sécurité à leur disposition, **52 %** des entreprises interrogées sont d'accord avec l'affirmation « **les environnements virtualisés prennent une place de plus en plus importante au sein de notre infrastructure informatique vitale** ». Ils doivent donc être efficaces et sûrs, mais il est clair qu'un effort de sensibilisation est nécessaire pour les protéger de manière efficace.

De manière générale, les entreprises qui mettent en place des environnements virtuels ne sont pas préparées aux changements nécessaires dans leur politique de sécurité, notamment le renforcement de leurs connaissances en matière de protection de la virtualisation et l'adoption de plates-formes de sécurité spécialisées. Ces deux points sont essentiels à la sécurité dans ce domaine.

Rapport sur les risques informatiques mondiaux 2014 :

5 Lutte contre les fraudes : l'évaluation du coût

La prévention des fraudes n'est pas loin des premières priorités des entreprises. **63 %** des personnes interrogées sont d'accord avec l'affirmation suivante : « **Nous mettons tout en œuvre pour faire en sorte que nos mesures de lutte contre les fraudes soient à jour** ». Ce chiffre est supérieur d'au moins **10 %** à ceux qui s'inquiètent de l'intégration mobile, de la virtualisation, des attaques DDoS et d'autres problématiques essentielles liées aux stratégies informatiques.

Toutefois, **43 %** des entreprises continuent de penser qu'elles doivent améliorer la façon dont elles protègent leurs transactions bancaires.

Cette inquiétude est malheureusement justifiée. En 2013, le nombre de cyber-attaques impliquant des programmes malveillants ciblant les données financières a atteint 28,4 millions, une hausse de 27,6 % par rapport à 2012[1]. Sur la même période, Kaspersky Lab a protégé 3,8 millions d'utilisateurs contre les attaques financières et bloqué plus de 330 millions d'attaques de phishing[2].

En 2013, le nombre de cyber-attaques impliquant des programmes malveillants ciblant les données financières a atteint 28,4 millions, une hausse de 27,6 % par rapport à 2012[1].

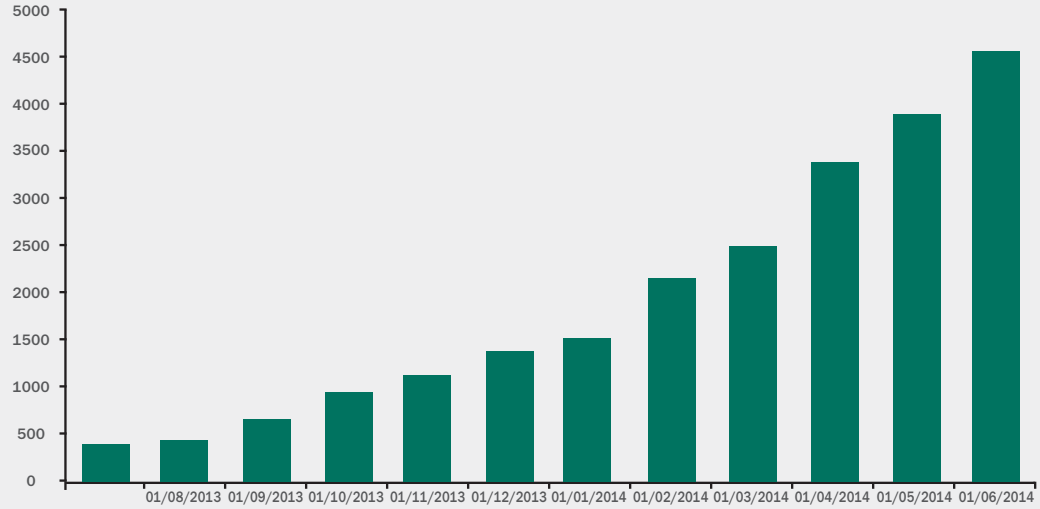
CHEVAUX DE TROIE CIBLANT LES DONNÉES BANCAIRES SUR MOBILE

Les programmes malveillants mobiles sont conçus pour enrichir les cyber-criminels. Ils fonctionnent aux côtés de chevaux de Troie Windows et contournent les techniques d'authentification classiques, en attaquant et en dérobant les numéros de transaction mobiles (mTAN) émis par les banques, permettant ainsi de réaliser des virements frauduleux.

Les chevaux de Troie bancaires autonomes sur Android ont connu une hausse soudaine et considérable au cours des 18 derniers mois, passant de seulement 67 début 2013 à 1 321 à la fin de l'année, et 3 215 supplémentaires ont été signalés à la mi-2014[3]. Bien que jusqu'ici, ces attaques aient essentiellement visé des utilisateurs en Russie et en CEI, il est probable que les cyber-criminels continueront de développer leurs techniques, afin d'étendre leur portée et de s'attaquer à de nouveaux marchés.

1. http://www.kaspersky.com/about/news/virus/2014/Kaspersky-Lab-statistics-attacks-involving-financial-malware-rise-to-28-million-in-2013
2. http://securelist.com/analysis/kaspersky-security-bulletin/59414/financial-cyber-threats-in-2013-part-2-malware/
3. http://securelist.com/analysis/quarterly-malware-reports/65340/it-threat-evolution-q2-2014/.

NOMBRE DE CHEVAUX DE TROIE CIBLANT LES DONNÉES BANCAIRES DÉTECTÉS AU 2ème TRIMESTRE 2014



Source : http://securelist.com/analysis/quarterly-malware-reports/65340/it-threat-evolution-q2-2014/

Les exemples les plus connus incluent ZeuS-in-the-Mobile (ZitMo), SpyEye-in-the-Mobile (SpitMo), Carberp-in-the-Mobile (CitMo) et Svpeng. Svpeng est un cheval de Troie Android qui dérobe les identifiants d'accès à une application de banque mobile. Il peut aussi dérober des informations sur la carte bancaire de l'utilisateur en l'invitant à saisir ses coordonnées bancaires à l'ouverture de Google Play. Au cours des trois mois d'existence de ce cheval de Troie, Kaspersky Lab en a découvert 50 variantes et bloqué plus de 900 installations[4].

Les marchés financiers reposent sur la confiance : confiance que les obligations seront honorées, que les paiements seront effectués et que les données seront protégées. Il n'est donc pas étonnant que la protection de l'image et des références soient des priorités essentielles pour les entreprises exerçant dans le domaine de la sécurité des données financières.

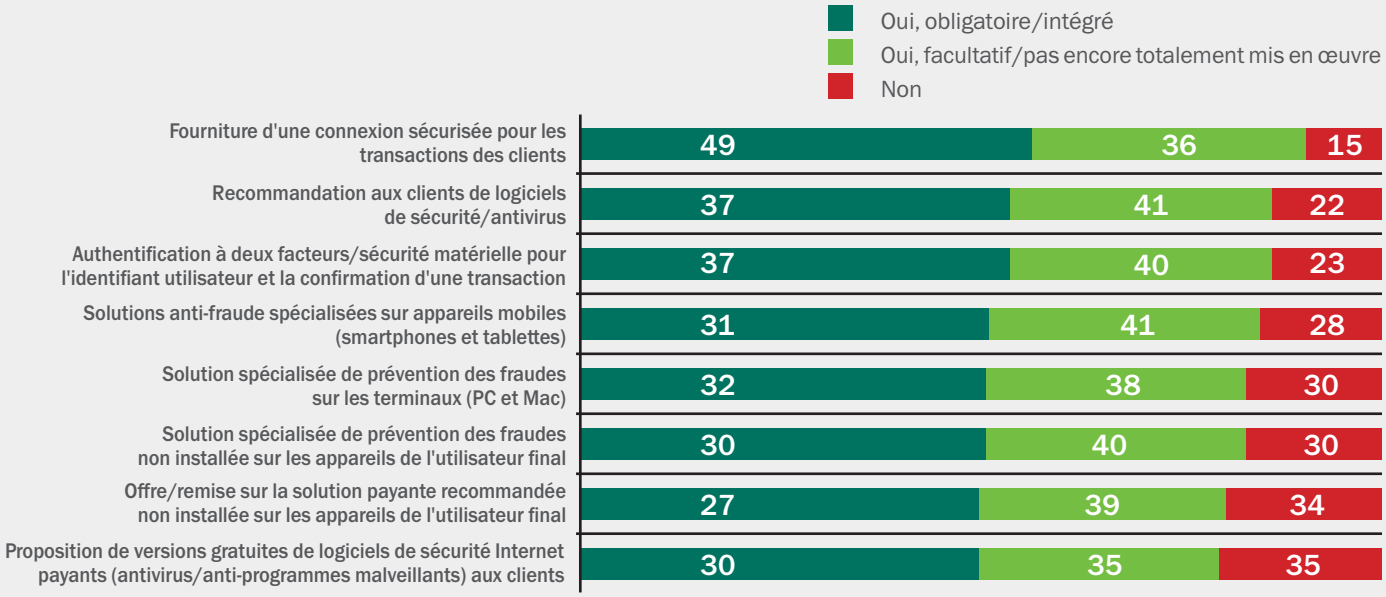
73 % des entreprises sont influencées par la réputation d'une banque en matière de sécurité lorsqu'elles décident avec qui travailler, et **82 %** se déclarent prêtes à changer de banque si la leur subissait un piratage de données. Cela n'a rien d'étonnant ; la prise en compte de la réputation d'une entreprise est une bonne pratique de gestion du risque. Il n'est pas plus étonnant que la protection des données des clients soit au cœur des priorités des entreprises interrogées. En revanche, il est intéressant de constater que **18 %** d'entre elles se déclarent prêtes à tolérer une faille dans leur propre système de sécurité financière.

Il est par ailleurs assez alarmant que plus de la moitié **(51 %)** de l'ensemble des entreprises interrogées considère que les mesures prises par les établissements financiers pour protéger leurs données sont suffisantes. Mais alors, que font au juste les prestataires de services financiers et marchands sur Internet pour protéger leurs clients et empêcher les fraudes ?

L'étude a interrogé plus de 2 500 entreprises travaillant dans ce secteur et les résultats indiquent pour la plupart que celui-ci est en phase de transition. Bien que près de la moitié des entreprises interrogées proposent une connexion sécurisée, environ un tiers d'entre elles n'a pas terminé la mise en œuvre de son service sécurisé ou ne l'applique pas, et **15 %** ne propose aucun service de ce genre. Pour les autres méthodes de protection des transactions, la plupart des entreprises sont soit en train de mettre en place des solutions dans ce domaine, en proposant des mesures anti-fraude en option, soit ne s'en sont pas encore occupé.

4. http://securelist.com/blog/research/57301/the-android-trojan-svpeng-now-capable-of-mobile-phishing/

MESURES DE LUTTE CONTRE LES FRAUDES APPLIQUÉES PAR LES PRESTATAIRES DE SERVICES FINANCIERS ET MARCHANDS SUR INTERNET



BASE : 2 680. Toutes les personnes interrogées travaillant dans les services financiers ou exerçant des activités commerciales en ligne

Les banques et leurs clients ne partagent pas le même point de vue concernant la responsabilité de la sécurité financière. Seulement **35 %** des clients pensent que les établissements financiers sont responsables de la sécurité financière, contre **85 %** des établissements eux-mêmes. Les TPE et petites entreprises sont les plus enclines à considérer que la responsabilité incombe à l'établissement financier – **avec 48 %** et **41 %** respectivement, contre seulement **27 %** chez les grands groupes.

Compte tenu du manque d'équipes de sécurité dédiées au sein des petites entreprises, le personnel informatique doit assumer seul le contrôle de la protection des processus et la responsabilité en cas de problème dans ce domaine. **28 %** des clients considèrent que la responsabilité finale incombe au service informatique. Cela souligne encore un peu plus le besoin d'une protection multi-niveaux et entièrement intégrée, capable de répondre à tous les besoins des PME.

> **Il existe un manque cruel de clarté concernant l'identification du responsable de la protection des transactions. La réponse est que les entreprises et les établissements financiers doivent en faire bien plus. Il s'agit de gestion du risque, et la situation actuelle laisse penser que l'exposition est excessive.**
>
> David Emm, Global Research & Analysis Team, Kaspersky Lab

Rapport sur les risques informatiques mondiaux 2014 :

6 Le coût réel du piratage des données

Que peut coûter un piratage de données à l'entreprise ? Sans avoir subi un tel désagrément, il n'est pas facile de répondre à cette question. Et quand c'est le cas, on ne sait que trop bien le prix que l'on a dû payer. Les répercussions d'un piratage de données sont toujours supérieures à la perte initiale d'informations sensibles et confidentielles, et les dégâts qu'il cause vont bien plus loin.

Les failles de sécurité entraînent souvent des frais supplémentaires, notamment des actions correctrices et préventives. Bien sûr, le pire dans l'immédiat est la peur que les informations confidentielles de l'entreprise soient tombées entre les mains de cyber-criminels, mais les répercussions durables peuvent inclure le coût de la perte de données, la dégradation de l'image de l'entreprise, la baisse de l'efficacité, les coûts externes, les dépenses liées aux actions correctrices et le manque à gagner.

Tout cela peut être catastrophique pour une entreprise. Parmi les sociétés interrogées ayant subi un piratage de données, **55 %** considèrent qu'il leur a été très difficile de reprendre leurs activités comme auparavant. Et il ne s'agit pas seulement de court terme. **54 %** des entreprises déclarent que la perte de données a eu un impact négatif sur leur réputation, détériorant l'image de fiabilité qu'elles avaient auprès de leurs clients, leurs actionnaires et les autres professionnels.

Les chiffres ci-dessous en disent plus sur la durée des perturbations qu'un piratage de données peut entraîner, et illustrent le nombre considérable d'entreprises ne pouvant plus exercer leurs activités ni gagner de l'argent.

La grande majorité des entreprises – **87 %** pour être précis – ne parvient pas à résoudre le problème seule, et doit demander de l'aide à des services professionnels : consultants en sécurité informatique, avocats, auditeurs ou encore cabinets-conseils spécialisés dans la gestion du risque. Près de la moitié de ces entreprises (**47 %**) déclare que ces services ont engendré des frais supplémentaires importants.

Mais les dépenses liées aux actions correctives ne se limitent pas aux services externes. Lorsqu'elles subissent un piratage de données, les PME peuvent dépenser jusqu'à 7 000 $ supplémentaires en recrutement, 6 000 $ en formation et 9 000 $ en systèmes. Et les groupes, certes plus grands mais pour lesquels les enjeux sont considérables, peuvent dépenser en plus jusqu'à 59 000 $ en recrutement, 35 000 $ en formation et 75 000 $ en systèmes.

> **Après une atteinte à la sécurité, la perte de données n'est que la partie immergée de l'iceberg financier. Le coût réel est bien supérieur. Il existe certains coûts tangibles évidents, comme les mesures de sécurité supplémentaires et les conseils juridiques, mais les dommages causés à l'image de marque et à la réputation sont sans doute encore plus importants.**
> Costin Raiu, Global Research & Analysis Team, Kaspersky Lab

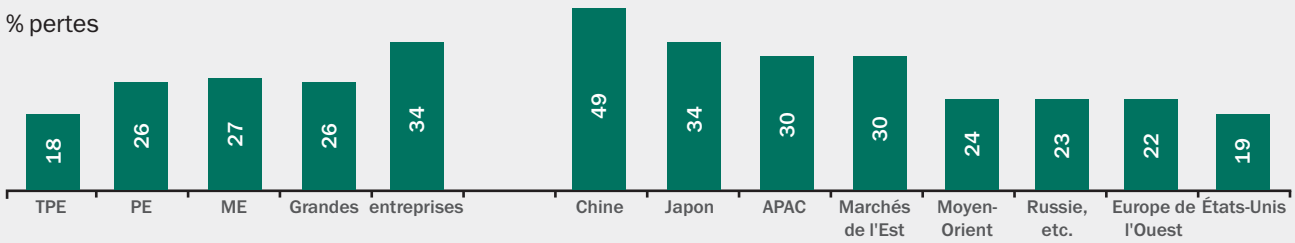
L'impossibilité d'exercer ses activités à la suite d'un piratage de données ou d'une attaque de sécurité est une autre source d'inquiétude majeure. C'est le cas d'environ un tiers des entreprises ayant subi une perte de données. Bonne nouvelle en revanche : entre 2013 et 2014, petites et grandes entreprises ont fait des progrès concernant la protection dans ce domaine, le coût moyen des périodes d'arrêt forcé ayant baissé comme illustré ci-dessous.

Taille des entreprises	Coût des périodes d'arrêt	
	2013	2014
PME	64 000 $	57 000 $
Grands groupes	1,7 M $	1,6 M $

Quels enseignements retirer de ces constatations ? En bref, que les dépenses engagées en aval sont toujours plus élevées que celles en amont. Les entreprises doivent donc désormais se demander si elles peuvent vraiment se permettre de ne pas se protéger.

Voilà une réponse intéressante à cette question. En moyenne, un peu plus d'un quart des entreprises (**26 %**) se disent prêtes à accepter une perte de données ou une atteinte à la sécurité. Pourquoi ? Parce qu'elles pensent que celle-ci leur coûtera moins que la mise à niveau de leurs systèmes informatiques nécessaires à la prévention de ce genre d'événement, comme illustré ci-dessous.

« Nous sommes prêts à assumer des pertes financières liées à la cyber-criminalité, car elles seront toujours inférieures au coût de mise à niveau de nos systèmes informatiques pour les prévenir. »



S'il serait certainement intéressant d'avoir accès aux calculs ayant conduit à cette conclusion, nous ne pouvons être d'accord avec celle-ci. En effet, les dégâts potentiels provoqués par les piratages de données vont bien au-delà du coût immédiat. La continuité des activités, l'image de marque, la réputation et les possibles coûts externes dépassent largement le coût financier d'une protection efficace et multi-niveaux.

7

Rapport sur les risques informatiques mondiaux 2014 :

Le problème de la gestion : dans un monde à la complexité croissante, il faut simplifier

L'étude de cette année a clairement mis en évidence la complexité pesant sur les entreprises de toutes tailles.

Celle-ci s'exerce sur deux plans :

1. Hausse de la complexité des menaces

Les programmes malveillants gagnent en complexité de plus en plus rapidement. Pour rester à l'abri, les entreprises doivent améliorer leur protection ; elles ne peuvent plus se contenter d'une simple solution antivirus. Cet état de fait a contribué à donner l'impression que les outils sont lourds et compliqués à gérer. Dans certains cas, cette impression est justifiée. Le marché de la sécurité pullule de produits de niche que les équipes informatiques en sous-effectif ont du mal à apprendre à utiliser, à intégrer et à gérer.

2. Hausse de la complexité de l'infrastructure informatique

Même les petites entreprises s'appuient sur une gamme étonnamment complexe de technologies. Les sociétés ont souvent plusieurs types de logiciels utilisés dans toute l'entreprise, et des collaborateurs qui installent des applications « sauvages » sur leurs systèmes. Si l'on y ajoute le développement de la virtualisation, on obtient un volume considérable d'éléments à surveiller et gérer. Mais c'est surtout la mobilité qui pose le plus de problèmes aux professionnels de l'informatique.

Que faire alors lorsque la tâche semble insurmontable ? Voici notre liste de recommandations :

Gérer un seul système de sécurité unifié

La difficulté que nous constatons le plus souvent, est que lorsqu'une nouvelle tâche apparaît (par exemple, l'application de correctifs), elle a tendance à provoquer l'achat impulsif d'une solution spécifique. Bien qu'à l'instant t, il puisse s'agir d'une bonne décision, avec le temps, cela provoque la création d'une série complexe de systèmes non reliés entre eux. En pratique, cela signifie davantage d'éléments à gérer, donc davantage de travail, et cela ouvre la voie à de nouvelles vulnérabilités (car il y a trop d'éléments à surveiller).

Inclure le mobile au projet général

Partez du principe que la majorité du personnel a un certain degré de mobilité dans son travail et vous serez dans le vrai. Là encore, un outil de sécurité mobile séparé signifie un élément supplémentaire à gérer, et de nouvelles vulnérabilités pesant sur la sécurité informatique en général.

Ajuster sa méthode : investir dans une protection multi-niveaux

Avec la hausse constante du nombre et de la sophistication des menaces, il est clair que nous sous-estimons à la fois l'ampleur et la gravité des problèmes de sécurité auxquels nous sommes confrontés. Intrusions sur le réseau, attaques de phishing et DDoS représentent toutes des menaces importantes, pouvant entraîner divers piratages de données très coûteux. Mais quelle est la vraie menace ? Ce sont toujours les programmes malveillants.

Compte tenu de cet état de fait, il est devenu crucial que les entreprises investissent dans une protection multi-niveaux. Le seul antivirus ne suffit plus. Les entreprises doivent adopter une approche bien plus proactive dans la gestion des comportements de programmes malveillants sophistiqués rôdant sur des sites en théorie sûrs, surgissant de fichiers en théorie innocents, qui exploitent les vulnérabilités des applications et profitent des appareils non protégés, voire d'un réseau Wi-Fi non sécurisé. Le volume de nouveaux programmes malveillants, associé à leur sophistication croissante, rend la protection proactive vitale. Il ne s'agit plus seulement d'un « petit plus ».

Ne pas se croire à l'abri des fraudes

Il n'est pas étonnant que la réputation d'une entreprise importe à ses clients. Ce qui l'est plus en revanche, c'est qu'un quart des entreprises interrogées considèrent que les mesures prises par les banques pour protéger leurs informations sont insuffisantes. Peut-être encore plus incroyable, 4 % des entreprises fournissant des services sur Internet n'appliquent aucune mesure particulière pour protéger leurs clients.

Ne jamais abandonner la formation des utilisateurs

En tant que professionnel de l'informatique, il vous incombe de vous assurer que vous disposez des bons outils et systèmes, et que vos collaborateurs sont correctement formés. Un employé peut permettre lui-même une atteinte à la sécurité, par manque d'information. Certes, la technologie est là pour l'en empêcher dans la plupart des cas. Mais si on l'associe à la formation et à des règles et stratégies vraiment strictes, les niveaux de sécurité informatique s'en trouvent décuplés.

Cela fait beaucoup, mais contrairement à ce que l'on pourrait croire, c'est loin d'être impossible à mettre en œuvre.

À la rencontre de nos experts

Les informations contenues dans ce rapport sont fournies par l'équipe Global Research and Analysis de Kaspersky Lab.

Costin Raiu
Costin est le directeur de l'équipe Global Research and Analysis. Anciennement Chief Security Expert, Costin travaille auprès de Kaspersky Lab depuis 2000. Il est spécialisé dans les sites Web malveillants, la sécurité des navigateurs et les failles d'exploitation, les programmes malveillants ciblant les services de banque en ligne, la sécurité des grandes entreprises et les menaces du Web 2.0. Lisez son blog sur la page http://securelist.com/author/costin/ ou suivez-le sur Twitter à l'adresse @craiu.

David Emm
David a fait ses premiers pas dans l'industrie anti-virus en 1990 et a rejoint Kaspersky Lab en 2004, où il a conçu et développé notre atelier sur la protection contre les programmes malveillants (Malware Defence Workshop). Il est actuellement Senior Regional Researcher pour le Royaume-Uni et il intervient régulièrement dans les médias en tant que commentateur. Ses principaux sujets de recherche portent sur l'écosystème des programmes malveillants, le vol d'identité, les aspects humains de la sécurité et les technologies Kaspersky Lab. Lisez son blog à la page http://securelist.com/author/davidemm/ ou suivez-le sur Twitter à l'adresse @emm_david.

Sergey Lozhkin
Senior Security Researcher, Global Research & Analysis Team, Sergey a rejoint Kaspersky Lab en 2012. Dans le cadre de son poste actuel, il effectue des recherches sur le cyber-espionnage, les analyses statiques et dynamiques des programmes malveillants, les réseaux Undernet tels que TOR, l'ingénierie sociale, les transferts de données sécurisés, l'analyse des vulnérabilités, les réseaux anonymes et la cyber-criminalité en général.

Avant de rejoindre Kaspersky Lab, Sergey a travaillé pour plusieurs entreprises en qualité de spécialiste des études de pénétration et des analyses de virus. Il a également enquêté sur plusieurs cyber-crimes.
Lisez son blog à la page http://securelist.com/author/sergeyl/ ou suivez-le sur Twitter à l'adresse @61ack1ynx.

PRENEZ DES MESURES SANS PLUS ATTENDRE : ESSAI GRATUIT DE 30 JOURS

Découvrez comment nos solutions de sécurité peuvent protéger votre entreprise des programmes malveillants et de la cyber-criminalité : essayez-les !

Téléchargez des versions complètes de nos produits et évaluez leur capacité à protéger parfaitement votre infrastructure informatique, vos terminaux et les données confidentielles de votre entreprise.

EFFECTUEZ UN ESSAI GRATUIT DÈS MAINTENANT

RETROUVEZ-NOUS SUR LES RESEAUX SOCIAUX

#securebiz

Visionnez nos vidéos sur YouTube

Rejoignez nos fans sur Facebook

Découvrex le blog d'Eugène Kaspersky

Suivez-nous sur Twitter

Retrouvez-nous sur LinkedIn

Plus d'informations sur : www.kaspersky.fr/business

À PROPOS DE KASPERSKY LAB

Kaspersky Lab est le plus grand éditeur privé mondial de solutions de protection des terminaux. La société fait partie des quatre principaux éditeurs mondiaux de solutions de sécurité pour utilisateurs de terminaux informatiques*. Depuis plus de 17 ans, Kaspersky Lab fait figure de précurseur dans le domaine de la sécurité informatique, fournissant des solutions de sécurité numérique efficaces aux grandes entreprises, PME et particuliers. Kaspersky Lab, dont la holding est enregistrée au Royaume-Uni, opère actuellement dans près de 200 pays et territoires du monde entier et offre une protection à plus de 300 millions d'utilisateurs. Plus d'informations sur : www.kaspersky.fr.

* L'entreprise a été classée quatrième fournisseur mondial de solutions de sécurité des terminaux, en termes de chiffre d'affaires, par IDC en 2012. Ce classement a été publié dans le rapport IDC « Worldwide Endpoint Security 2013–2017 Forecast and 2012 Vendor Shares » (Sécurité des terminaux dans le monde : prévisions pour 2013-2017 et parts de marché des fournisseurs en 2012), document numéro 242618, août 2013. Ce rapport classait les fournisseurs de logiciels selon leurs revenus provenant des ventes de solutions de sécurité des terminaux en 2012.