KASPERSKY lab

ENQUÊTE SUR LES RISQUES INFORMATIQUES MONDIAUX

2015

http://www.kaspersky.fr/entreprise-securite-it/
#EnterpriseSec

Rapport de l'enquête sur les risques informatiques mondiaux: point sur la situation actuelle

Publiée pour la cinquième année consécutive, le rapport basé sur l'enquête annuelle de Kaspersky Lab sur les risques informatiques au niveau mondial contient 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 par l'équipe d'experts en cybersécurité 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

L'enquête en quelques mots :

- 5 564 entreprises interrogées
- 38 pays
- Période couverte : avril 2014 - mai 2015
- Personnes interrogées : professionnels de l'informatique ayant de « bonnes connaissances » des problèmes informatiques

Résumé analytique

Cette année a été marquée par un nouveau déferlement de cyberattaques de haut vol dont les médias se sont fait l'écho. Ces attaques ont renforcé la prise de conscience parmi les entreprises que, parallèlement à ces attaques médiatisées, il existe un large spectre de menaces plus discrètes tout aussi dangereuses pour leurs activités.

Plus particulièrement, les entreprises sont de plus en plus conscientes qu'elles ne sauraient se préoccuper que de leur seule sécurité dans notre monde hyper-connecté. La vulnérabilité des tierces parties, en particulier celles liées aux transactions financières, a donc rejoint leur liste de priorités.

Ainsi, parmi les entreprises interrogées cette année, **72 %** étudient soigneusement les antécédents d'une banque en matière de sécurité avant de décider de collaborer avec elle. En outre, **90 %** des grandes entreprises seraient disposées à payer des frais supplémentaires pour sécuriser davantage leurs transactions.

Évidemment, l'argent est loin d'être la seule ressource à protéger. Au fur et à mesure que le paysage informatique change et que de plus en plus de données sont transférées hors des entreprises auxquelles elles appartiennent, les sociétés s'inquiètent du fait que les fournisseurs SaaS ne prennent pas suffisamment de mesures pour sécuriser ces données. Il s'agit d'un problème que **37 %** des entreprises interrogées ont cité comme une source d'inquiétude.

À certains égards, cette prise de conscience des menaces s'est accompagnée d'une réponse proactive. On a ainsi constaté une hausse de **15 %** du déploiement de logiciels de lutte contre les programmes malveillants et **66 %** des entreprises sont maintenant protégées par la mise en œuvre d'une solution de sécurité complète.

Toutefois, elles sont encore nombreuses à opter pour une approche standardisée, plutôt qu'une stratégie décloisonnée qui tient compte de la nécessité d'une protection spécialisée. Ainsi, l'utilisation de logiciels de lutte contre les programmes malveillants sur les appareils mobiles est en baisse de **8 %** et seulement **26 %** des personnes interrogées utilisant un environnement virtualisé protègent ce dernier à l'aide d'une solution sur mesure.

Ce manque d'investissement semble être dû à une sous-estimation de l'intérêt de se protéger. Mais ce n'est pas nouveau. L'importance de la sécurité se mesure toujours après coup, et de nombreuses organisations ne réalisent pas à quel point une violation de données pourrait leur porter préjudice. Le coût moyen d'une violation de données pour les **PME** et les **grandes entreprises** s'élève à **38 000 $** et **551 000 $** respectivement, et **60 %** des entreprises victimes d'une atteinte à la sécurité souffrent de dysfonctionnements importants.

Il est temps pour les entreprises de repenser leurs budgets en matière de sécurité. Considérée séparément de l'infrastructure informatique, la sécurité est une dépense difficile à justifier avant l'apparition d'une catastrophe. En revanche, lorsqu'elle est perçue comme une composante essentielle de l'environnement informatique (appareils mobiles et machines virtualisées inclus), son importance devient évidente, surtout lorsque l'on considère les dommages et les coûts considérables qu'elle est en mesure de prévenir.

L'éclairage de l'équipe GReAT

« L'attaque Carbanak, découverte début 2015, a clairement mis au jour le fait que les cybercriminels concentrent désormais leurs efforts sur les institutions financières ainsi que d'autres types d'entreprises. »

Perception et réalité

En tant que décideur informatique, il vous incombe de préserver la sécurité du réseau informatique de votre entreprise. Votre tâche consiste à protéger les données sensibles et à caractère privé, ainsi qu'à préserver les actifs de votre entreprise sur les appareils physiques, virtuels et mobiles.

On peut dire avec certitude que la sécurité est au cœur des priorités des entreprises de toutes tailles à travers le monde. Dans notre rapport de l'enquête sur les risques informatiques mondiaux, **50 %** des professionnels de l'informatique ont cité la sécurité parmi leurs trois préoccupations principales. Mais sont-ils satisfaits de leur niveau actuel de protection informatique ? Pas vraiment. Près de la moitié des sociétés interrogées (**47 %**) estiment que leur sécurité informatique ne répond pas à leurs attentes pour ce qui est de sécuriser leurs transactions financières.

Au cours des 12 derniers mois, les entreprises ont considérablement renforcé leur utilisation de logiciels antivirus et de lutte contre les programmes malveillants, beaucoup d'entre elles déclarant être désormais « entièrement » protégées. Et les grandes entreprises réagissent déjà à la nécessité d'adopter une plus large gamme de mesures de sécurité.

Rien d'étonnant à cela lorsque l'on sait que **32 %** des entreprises estiment avoir fait l'objet d'une attaque ciblée, dans le passé ou au moment de cette enquête. En d'autres termes, près d'une société sur trois craint d'avoir subi une violation de données, soit une hausse de **7 %** par rapport à la même époque l'an dernier. Ce résultat est à mettre en corrélation avec le fait que **52 %** des participants pensent également que leur organisation a besoin d'améliorer ses plans de réaction aux incidents pour les violations de données et autres événements de sécurité informatique.

Actuellement, **46 %** des entreprises estiment que le nombre d'attaques à l'encontre de sociétés comme la leur est en hausse, soit une baisse de **3 %** par rapport à l'année dernière. Davantage de personnes pensent que le nombre d'attaques n'a pas changé, **44 %** cette année contre **39 %** l'année dernière. Et **10 %** considèrent que le nombre d'attaques a baissé, contre **11 %** les deux années précédentes. En outre, les attaques de cryptovirus perçues visant nos sondés sont en hausse, de **37 %** à **45 %** par rapport à l'année passée.

Il existe bien sûr des contrastes au sein des données. De manière générale, les professionnels de l'informatique en Russie et en Chine ne perçoivent pas d'accroissement de la dangerosité du paysage des menaces, contrairement à ceux des marchés émergents, qui ressentent une aggravation de la menace.

47 % des entreprises souhaitent que les banques améliorent la sécurité des transactions en ligne. Selon elles, les banques n'en font pas assez pour sécuriser les paiements et elles craignent que des cybercriminels ne puissent pirater leur infrastructure et dérober des fonds. Elles perdent peu à peu confiance dans ce qui devrait être le moyen le plus simple, le plus sûr et le plus pratique d'envoyer et de recevoir de l'argent.

Plus inquiétant encore, la confiance s'effrite de plus en plus entre les entreprises et les fournisseurs SaaS tiers. **37 %** des sondés craignent que ces plateformes ne soient pas sécurisées et fournissent un moyen facile pour les cybercriminels d'infiltrer leur réseau informatique. Il s'agit d'une augmentation de **4 %** par rapport à l'année dernière et ce pourcentage risque encore de progresser alors que les entreprises sont de plus en plus nombreuses à migrer leurs opérations quotidiennes dans le cloud.

Sur ce sujet des interférences extérieures, **42 %** se disent préoccupés par l'intrusion croissante de l'État dans leur infrastructure informatique. Ce chiffre est en hausse de **4 %** cette année et est particulièrement élevé en Chine (**50 %**), sur les marchés de l'Est (**46 %**) et dans la région APAC (**50 %**).

Niveaux de menace : allons-nous dans la bonne direction ?

Commençons par les mauvaises nouvelles. Au cours de l'année passée, plus de **90 %** des entreprises ont subi une forme de menace externe. La gravité de ces menaces varie de mineure à extrême, mais pour une entreprise en activité aujourd'hui, il s'agit d'une statistique très troublante.

22 % des entreprises ont perdu des données du fait d'une menace extérieure. Mais la bonne nouvelle, c'est qu'on a recensé moins de cas de vols et de programmes malveillants « évidents » l'année dernière que l'année précédente. De plus, le nombre d'organisations ayant perdu des données du fait d'un programme malveillant a reculé de **33 %** à **25 %**.

L'éclairage de l'équipe GReAT

« Alors que les gros titres de l'actualité relatent principalement les attaques visant les grandes organisations, les entreprises de toutes tailles sont en réalité des victimes potentielles des cybercriminels, qui cherchent à s'approprier la propriété intellectuelle, à voler les données des clients ou à s'implanter dans une autre société faisant affaire avec l'entreprise victime. »

Évolution de la nature des attaques

Au cours de la même période, 9 % des entreprises ont connu des attaques ciblées, un chiffre qui s'élève à 15 % dans les grandes entreprises, et plus de la moitié d'entre elles (53 %) ont signalé une perte de données sensibles suite à ces attaques.

Cependant, les entreprises sont **4 %** de moins à avoir signalé des attaques par phishing, **3 %** de moins des intrusions dans les réseaux ou du piratage, et **9 %** de moins des vols d'appareils mobiles par une personne externe. En fait, hormis quelques cas seulement où les attaques perçues sont restées stables ou ont augmenté de un ou deux pour cent, les attaques ont diminué partout dans le monde.

En Chine et en Europe de l'Ouest, le vol d'appareils mobiles par une personne externe a chuté de **12 %**. En Amérique du Nord, la baisse perçue de **10 %** des programmes malveillants de tous types est la deuxième plus élevée dans le monde après la Chine avec **13 %**.

Le recul des vols d'appareils mobiles est peut-être dû à un meilleur chiffrement mis en œuvre sur les dispositifs mobiles au cours de l'année écoulée. Quant à la diminution perçue des programmes malveillants, elle s'explique probablement par le fait que les entreprises ne se rendent tout simplement pas compte de la perte de données subie, grâce aux techniques de plus en plus complexes et furtives déployées par les cybercriminels. Malgré tout, les sondés sont **54 %** à se dire bien plus préoccupés par la sécurité des appareils mobiles qu'ils ne l'étaient il y a un an.

> **54 %** des sondés se disent malgré tout bien plus préoccupés par la sécurité des appareils mobiles qu'ils ne l'étaient il y a un an.

Intéressons-nous maintenant aux menaces internes. **21 %** des entreprises ont perdu des données sensibles en raison de menaces internes au cours de l'année écoulée. Et **73 %** ont subi un incident de sécurité interne en 2015. Les menaces les plus courantes ont été causées par des vulnérabilités logicielles et des actions accidentelles du personnel, y compris la fuite ou le partage accidentels de données. **30 %** des sondés ont admis avoir subi des menaces liées à des vulnérabilités de logiciels existants.

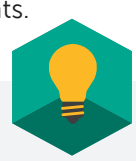
> **73 %** des entreprises ont subi un incident de sécurité interne en 2015.

Mais les problèmes ont peut-être des racines plus profondes, **46 %** des personnes interrogées doutant du fait que les cadres dirigeants (en dehors du service informatique) comprennent bien les risques de sécurité informatique auxquels leur entreprise est exposée.

> **46 %** des personnes interrogées doutent du fait que les cadres dirigeants (en dehors du service informatique) comprennent bien les risques de sécurité informatique auxquels leur entreprise est exposée.

Il y a aussi de bonnes nouvelles dans ce domaine. Les fuites ou partages accidentels de données ont diminué de **6 %** au cours de la dernière année et les incidents dus à des logiciels vulnérables ou connaissant des dysfonctionnements sont en baisse de **2 %** par rapport à l'année dernière et de **8 %** par rapport à il y a deux ans. Quant à la perte de données à partir d'appareils mobiles volés ou perdus, elle a reculé de **7 %**. La baisse des vols semble indiquer que les employés sont de plus en plus prudents avec les appareils fournis par leur société lors de leurs déplacements.

Il faut toutefois signaler un nouveau problème qui concerne la confiance entre les entreprises et les fournisseurs tiers auxquelles elles recourent. On observe une forte tendance à la hausse des entreprises signalant des incidents de sécurité impliquant ce type de partenaires, en particulier dans les secteurs avec des niveaux élevés d'externalisation, tels que l'informatique ou la fabrication.



L'éclairage de l'équipe GReAT

« Non seulement le nombre d'attaques ciblées croît toujours, mais, plus inquiétant, les méthodes et les compétences des personnes qui les développent s'améliorent chaque année. Les attaques deviennent de plus en plus difficiles à détecter et il est parfois presque impossible de s'en débarrasser. »

Notre action : une prise de conscience lente

Les entreprises d'aujourd'hui font face à un nombre croissant de menaces élaborées par des cybercriminels de plus en plus astucieux, déterminés à déjouer la vigilance de leurs victimes de manières toujours plus complexes.

Le problème pour ces sociétés, c'est qu'utiliser une solution standardisée n'est plus suffisant pour se défendre contre les menaces d'aujourd'hui : les attaques sur les réseaux informatiques sont tout simplement trop puissantes et permanentes.

Les programmes malveillants constituent un problème particulièrement persistant. Leur évolution rapide et quotidienne les rend très difficiles à combattre. Mais de plus en plus d'entreprises sont mieux informées à leur sujet, raison pour laquelle on a constaté l'année dernière une hausse de **15 %** des logiciels de lutte contre les programmes malveillants déployés sur les postes de travail. **66 %** des entreprises actuelles sont maintenant protégées par une solution de sécurité complète.

> Au cours de la dernière année, le déploiement de logiciels contre les programmes malveillants sur les postes de travail a augmenté de **15 %**.

Avec le développement du travail mobile, les entreprises ont été contraintes de s'intéresser sérieusement au déploiement de solutions de sécurité mobile. La prolifération des smartphones et tablettes, et par conséquent leur ciblage par les cybercriminels, a mis leur protection au cœur des priorités des décideurs informatiques du monde entier.

Bien que la mise en œuvre de la gestion des appareils mobiles reste encore faible à **20 %**, son importance est reconnue par **44 %** des professionnels de l'informatique, soit une augmentation de **9 %** par rapport à l'année dernière.

Pourtant, le déploiement de solutions contre les programmes malveillants sur les appareils mobiles a chuté de **8 %**. Pourquoi donc ? Principalement parce que les entreprises ont « partiellement » mis en œuvre une solution, qui leur paraît suffisante pour protéger leurs employés sans avoir à déployer une protection « complète ».

Pour certains, il y a aussi le sentiment que la protection contre la perte de données n'en vaut pas le coût. **23 %** des entreprises ont estimé qu'il était simplement trop coûteux de justifier l'investissement, tandis qu'elles sont **33 %** à déclarer ne pas avoir suffisamment de données pour justifier sa mise en œuvre.

Et pour les entreprises ayant déjà fait l'investissement, seulement **31 %** jugent que cela leur a été utile. Un chiffre très faible, mais que l'on imagine monter en flèche si ces logiciels venaient à la rescousse des entreprises victimes d'une violation. Il est parfois difficile de quantifier un investissement tant qu'il n'a pas été utilisé.

17 % des entreprises externalisent actuellement leur prise de décisions en sécurité informatique à une personne ou société tierce, préférant le recours à des compétences externes au recrutement d'un spécialiste informatique de facto en interne. Et parmi les grandes entreprises, **42 %** utilisent maintenant des services de formation à la sécurité informatique pour rester maîtresses de leur sécurité, tandis que **41 %** utilisent des services d'investigation sur les incidents à la suite d'un événement. Ces chiffres montrent bien combien les grandes entreprises prennent au sérieux la sécurité informatique ; elles tiennent absolument à rester au fait des dernières technologies dans le domaine de la sécurité informatique.

La virtualisation, pas encore une priorité

La protection des architectures virtualisées aide les entreprises à atteindre une haute densité de virtualisation et à maintenir leurs performances, ce qui leur permet d' obtenir plus facilement un meilleur retour sur investissement.

La virtualisation fait depuis longtemps partie de la stratégie informatique de nombreuses sociétés, mais son taux de mise en œuvre réel reste faible.

Elle est visiblement présente à l'esprit de beaucoup des sondés, **53 %** des entreprises se disant très préoccupées par la protection de leurs environnements virtualisés. Et **89 %** ont déclaré que le fait de disposer de logiciels de sécurité avait un impact positif sur les performances de leurs machines virtuelles.

> **53 %** des entreprises sont très préoccupées par la protection de leurs environnements virtualisés.

Mais il existe un écart entre ce niveau de préoccupation et la volonté des entreprises de passer à l'action. La protection de l'infrastructure virtuelle fait partie des trois principales priorités de seulement **19 %** des décideurs informatiques, tandis que **22 %** citent la protection de l'infrastructure cloud.

En fait, les solutions de sécurité virtuelles entièrement déployées sont rares ; seules **26 %** des entreprises avec une infrastructure virtualisée y recourent. Et une majorité des sociétés, **56 %**, préfèrent gérer les menaces associées quand elles surviennent.

Pourquoi donc ? La virtualisation est un problème extrêmement complexe. Même les professionnels de l'informatique aguerris qui possèdent des connaissances pointues peuvent éprouver des difficultés à profiter des options à leur disposition. Seul un tiers des organisations possèdent une solide connaissance de chaque solution et environ un quart d'entre elles les comprennent peu ou pas du tout.

L'une des principales raisons pour lesquelles les professionnels de l'informatique n'utilisent pas de solution de sécurité spécialisée n'est autre que le fait qu'ils estiment que leur sécurité actuelle, non spécialisée, fonctionne suffisamment bien. **31 %** n'ont rencontré aucun problème avec leur anti-virus traditionnel, et ne voient donc pas la nécessité d'une mise à niveau. Et **27 %** des sociétés ayant rencontré des problèmes avec des produits traditionnels dans des environnements virtualisés pensent que ces problèmes ne nécessitent pas d'investir dans un système différent. En conséquence, elles sacrifient leurs performances pour des raisons d'économie, en utilisant des solutions qui ne sont pas adaptées aux environnements virtuels.

L'éclairage de l'équipe GReAT

« Il est vraiment important que les organisations maîtrisent la protection des environnements virtuels. Malgré une prise de conscience croissante des risques existants, on constate encore une inertie et un manque de compréhension des facteurs particuliers impliqués dans la protection des systèmes virtualisés. »

Lutte anti-fraude : chaque transaction doit être sécurisée

La prévention de la fraude est l'une des préoccupations les plus importantes en matière de sécurité pour toute entreprise. Elle contribue non seulement à protéger les transactions financières d'une entreprise, mais elle préserve également son image et la satisfaction des clients, pour qu'ils continuent de traiter avec elle en toute confiance.

Près des deux tiers des entreprises (**63 %**) ont déclaré qu'elles font tous les efforts possibles pour s'assurer que leurs mesures de sécurité sont à jour.

Il n'a jamais été plus important de protéger les transactions financières. Dans notre monde qui fait un usage intensif des appareils en tout genre, les cybercriminels peuvent exploiterles nouvelles façons de travailler. Alors que **64 %** de la main-d'œuvre utilise un ordinateur de bureau avec une connexion filaire et **50 %** un ordinateur de bureau avec une connexion wifi, les utilisateurs de smartphones à des fins professionnelles sont également nombreux : **27 %** les utilisent pour se connecter à des réseaux wifi et **18 %** les utilisent en déplacement grâce aux données mobiles.

> **72 %** des entreprises étudient les antécédents d'une banque en termes de sécurité avant de décider ou non d'établir le contact.

En raison du développement des services bancaires mobiles, les institutions financières sont témoins d'une augmentation de la fraude en ligne. Mais **48 %** de ces organisations déclarent que toutes les mesures qu'elles prennent visent davantage à atténuer ce problème qu'à le résoudre. Pour **29 %** d'entre elles, il est moins coûteux et plus efficace de gérer ces problèmes à mesure qu'ils surviennent, plutôt que d'essayer de les anticiper. Les banques semblent donc beaucoup plus enclines à engager des dépenses pour des actions correctives plutôt qu'à prendre des mesures préventives.

Or, il s'agit peut-être d'une attitude à court terme. Une banque qui protège ses clients et préserve les entreprises des dangers aura toujours la faveur des clients potentiels. **72 %** des entreprises étudient les antécédents d'une banque en termes de sécurité avant de décider ou non d'établir le contact.

Mais qui est finalement responsable ? **29 %** des banques et des services de paiement considèrent que la responsabilité incombe à leur propre département informatique, et pas du tout au client. Mais quand on leur demande s'ils prennent actuellement des mesures pour protéger leurs clients de la fraude liée aux transactions financières, seuls **67 %** répondent que la mise à disposition d'une connexion sécurisée est obligatoire.

Les banques ne sont pas les seules à devoir améliorer leur sécurité. **48 %** des entreprises ont indiqué qu'elles devaient améliorer la sécurité de leurs transactions financières. En fait, la plupart des entreprises estiment que la responsabilité ultime de la sécurité financière leur incombe à elles, et non à la banque. De plus, **90 %** des entreprises comptant plus de 250 employés seraient prêtes à payer pour bénéficier d'une sécurité renforcée si cela pouvait leur assurer des transactions financières plus sécurisées. Les entreprises de la région APAC, y compris la Chine et le Japon, seraient plus enclines à payer que celles des régions occidentales, qui accordent moins d'importance à leur réputation en termes de sécurité.

> **90 %** des entreprises comptant plus de 250 employés seraient prêtes à payer pour bénéficier d'une sécurité renforcée si cela pouvait leur assurer des transactions financières plus sécurisées.

L'éclairage de l'équipe GReAT

« Il est étonnant que malgré l'augmentation des fraudes en ligne signalées, de nombreuses banques pensent encore à tort qu'il revient moins cher de gérer les attaques quand elles se produisent, plutôt que de les anticiper. »

Violations de données : des coûts visibles et des conséquences invisibles

Il peut être difficile pour une entreprise de mesurer l'ampleur d'une atteinte à la sécurité avant qu'elle ne survienne. Une simple perte de données à première vue peut en réalité entraîner des dommages à long terme considérablement plus coûteux, et pas seulement en termes monétaires.

La prévention ou la gestion d'une atteinte à la sécurité informatique est une préoccupation majeure des professionnels de l'informatique dans tous les pays, mais les marchés de l'Est et le Japon en font à **50 %** leur inquiétude numéro un, devant tout le reste. Ce problème apparaît plus urgent que la compréhension des différentes technologies de sécurité sur le marché (numéro deux) et la gestion des changements dans les systèmes et l'infrastructure informatiques (numéro trois). Cette préoccupation n'arrive pas au premier rang pour les seules grandes entreprises, elle est en première position chez les très petites entreprises également.

Une atteinte à la sécurité peut entraîner le vol d'actifs, des fuites de données, mais aussi ternir la réputation d'une entreprise. Et les méthodes pour remédier à certains des dangers (frais d'avocat et de conseil, dépenses liées aux actions correctives...) sont coûteuses et mobilisent un temps considérable. **57 %** des entreprises attaquées ont dû s'acquitter de frais supplémentaires importants.

Une violation de données représente également un énorme pas en arrière pour ce qui est de maintenir le fonctionnement d'une entité commerciale. Les processus et pratiques standards sont compromis, ce qui peut entraîner un arrêt des activités de l'entreprise ou de graves pertes de performance. **60 %** des entreprises ayant subi une violation de données ont ensuite connu de graves dysfonctionnements.

Les attaques les plus dangereuses, celles qui ont infligé le plus de dommages, sont les attaques par phishing, les intrusions sur les réseaux et le cyberespionnage. Des services professionnels coûteux sont habituellement nécessaires pour rétablir un service normal à la suite de ces attaques.

Pour les PME, les temps d'arrêt ainsi causés ont entraîné des pertes d'opportunités commerciales à hauteur de 16 000 $ en moyenne. Les grandes entreprises ont quant à elles accusé une perte moyenne de 203 000 $. Mais lorsqu'un programme malveillant empêche une entreprise de fonctionner correctement, les conséquences peuvent être stupéfiantes. En 2015, les temps d'arrêt dus à des attaques ont coûté en moyenne 1,4 million de dollars aux grandes entreprises. Un chiffre cependant en baisse par rapport à 2014 (1,5 million de dollars). Pour les PME, le coût des temps d'arrêt a en revanche augmenté, passant de 52 000 $ l'an dernier à 66 000 $ aujourd'hui. Alors, comment les grandes entreprises parviennent-elles à réduire leurs pertes ? La plupart ont pris en compte la possibilité d'une attaque et se sont préparées avec de meilleurs outils de reprise après sinistre, plus efficaces.

Au cours de l'année passée, **87 %** des incidents de perte de données ont requis l'intervention de professionnels tiers pour résoudre le problème : consultants en sécurité informatique, avocats ou encore cabinets-conseils spécialisés dans la gestion du risque.

Et ce n'est pas tout. **56 %** des événements de perte de données ont entraîné une atteinte à l'image et à la réputation de l'entreprise en question. Étant donné le grand nombre de facteurs impliqués, il est difficile de chiffrer précisément l'impact financier de ce type d'atteinte à l'image de marque.

En tenant compte d'éléments tels que l'argent dépensé pour rétablir la réputation et la perte de chiffre d'affaires consécutive aux résiliations de contrats ou aux opportunités manquées, il est néanmoins possible d'estimer le coût médian d'une violation de données pour les PME à **11 000 $** ; pour les grandes entreprises, ce chiffre est bien plus important et s'élève à **84 000 $**. Un événement grave de perte de données coûte en moyenne autour de **38 000 $** à une PME, tandis qu'une grande entreprise est confrontée à une perte considérable de **551 000 $**.

Les dépenses moyennes estimées consacrées à des activités correctives se sont élevées à **8 000 $** pour les PME, alors que les grandes entreprises ont dépensé **69 000 $** par incident. Mais les dépenses liées aux actions correctives ne se limitent pas aux services externes. Les entreprises de toutes tailles peuvent potentiellement dépenser des milliers de dollars pour embaucher du personnel supplémentaire, former leurs collaborateurs et acquérir de nouveaux systèmes informatiques.

Ces sommes sont alarmantes. Reste que pour les PME, du moins, les chiffres évoluent dans la bonne direction. L'impact global total, qui tient compte de toutes les pertes et dépenses supplémentaires, a chuté de **12 %**. Malheureusement, la situation se présente un peu moins bien pour les grandes entreprises. En moyenne, l'impact global total a augmenté de **14 %**. Les violations de données impliquant des environnements virtuels ont été deux fois plus coûteuses en moyenne que les autres, avec des chiffres s'élevant à **34 000 $/74 000$** pour les PME et **454 000 $/942 000 $** pour les grandes entreprises.

Ce qui est évident, c'est que pour une entreprise qui reste ébranlée par une attaque, il aurait été bien moins coûteux d'investir dans une solution de sécurité efficace en premier lieu.

L'éclairage de l'équipe GReAT

« Ne vous croyez pas à l'abri. Il existe de nombreux exemples de grandes entreprises qui ont été mises en liquidation après une violation de données en bonne et due forme. Le coût des actions correctives est largement supérieur à celui de la prévention. »

Attaques DDoS : une menace multiforme

Les attaques par déni de service distribué (DDoS) sont lancées dans le but de mettre hors service la présence en ligne ou les processus clés de l'organisation ciblée. Les dommages, et les coûts connexes, peuvent être considérables et durables.

Si les attaques DDoS existent depuis longtemps déjà, elles sont actuellement plus dangereuses qu'elles ne l'ont été au cours des dernières années. Le coût du lancement d'une attaque DDoS a également diminué, ce qui a contribué à l'accroissement rapide du volume des attaques. Les attaques d'aujourd'hui sont par ailleurs plus complexes, rendant la défense beaucoup plus difficile.

Parmi les entreprises interrogées, **50 %** ont connu un certain degré de perturbation dû à une attaque DDoS au cours de l'année passée. Très souvent, une attaque DDoS est combinée à une atteinte à la sécurité, pour un impact accru. L'année dernière, **45 %** des attaques DDoS ont été combinées avec des programmes malveillants, **32 %** avec une intrusion sur les réseaux ou un piratage, et **26 %** avec une fuite de données.

> Parmi les entreprises interrogées, **50 %** ont connu un certain degré de perturbation dû à une attaque DDoS au cours de l'année passée.

Quels types d'entreprises ont été les plus touchées ? Parmi les entreprises comptant plus de 10 employés, **24 %** des banques ont été victimes d'une attaque, tout comme **23 %** des sociétés de télécommunications et **20 %** des entreprises de services financiers. Au bas de l'échelle, **7 %** des sociétés de médias et de divertissement, **8 %** des sociétés d'immobilier et **11 %** des organismes de soins de santé ont également souffert d'une attaque.

Le site Web public des entreprises a été le service le plus fréquemment touché par une attaque DDoS, près de la moitié des entreprises sondées (**47 %**) citant l'incapacité de leur site Web à fonctionner normalement. Pour **38 %**, le portail client ou la zone de connexion a été le deuxième composant le plus touché, tandis que les problèmes avec les services de communication (**37 %**) arrivent en troisième position.

Le ralentissement du chargement des pages a été la forme de perturbation la plus courante pour les entreprises. Elles sont **58 %** à avoir connu des temps de chargement des pages significativement plus longs, **34 %** ayant trouvé que les temps de chargement des pages étaient légèrement allongés. **43 %** ont connu des retards d'une journée ou plus, certaines pages prenant au moins plusieurs semaines à charger. **24 %** ont également connu une interruption complète de leurs services.

Les entreprises craignent de nombreuses conséquences d'une attaque DDoS. **27 %** ont déclaré que leur plus grande crainte était un temps d'arrêt nuisant à leur réputation auprès des clients. **27 %** ont également répondu qu'elles craignaient en premier lieu une indisponibilité des ressources en ligne, susceptible de conduire à une perte de revenus ou d'opportunités commerciales. La deuxième crainte relevée (**16 %**) concerne les coûts encourus pour combattre l'attaque et restaurer le fonctionnement normal des services. En troisième place, à **15 %**, les sondés ont cité la possibilité de perdre des clients suite à une attaque.

Mais à qui la responsabilité de gérer la menace d'attaques DDoS incombe-t-elle ? Dans les petites entreprises, la responsabilité incombe le plus souvent à la direction et à des fournisseurs de services externes. Mais dans les grandes entreprises, la responsabilité échoit au département informatique ou de sécurité interne.

Les avis à l'égard des attaques DDoS sont pour le moins partagés. Seuls **56 %** des professionnels de l'informatique jugent justifié de dépenser de l'argent afin de prévenir ou d'atténuer une future attaque. Seuls **52 %** ont déclaré qu'ils s'estimaient bien informés au sujet des attaques DDoS, tandis que **48 %** ont déclaré connaître l'identité et les motivations des auteurs des attaques DDoS récentes dont ils ont fait l'objet.

À la question de savoir qui ou ce qu'elles suspectaient être à l'origine de l'attaque DDoS qu'elles avaient subie, les entreprises ont désigné toutes sortes d'agresseurs potentiels, les criminels étant le groupe le plus souvent accusé. **28 %** des professionnels de l'informatique estiment avoir été victimes de criminels cherchant à perturber leurs activités. **18 %** considèrent qu'il s'agissait de criminels cherchant à les perturber ou à les distraire tandis qu'une autre attaque était orchestrée. Et **17 %** ont répondu qu'il s'agissait de criminels utilisant l'attaque pour prendre la société en otage.

En dehors des criminels, **12 %** pensent que les attaques ont été lancées par leurs concurrents, dans le but d'obtenir un avantage sur le marché ou de voler des informations privées. Les sondés en Russie et en Chine se montrent les plus soupçonneux à l'égard de leurs concurrents. **11 %** des sociétés soupçonnent également des militants politiques d'être à l'origine de l'attaque, tandis que **5 %** pensent qu'il pourrait s'agir du gouvernement ou de pouvoirs de l'État.

L'éclairage de l'équipe GReAT

« Les entreprises doivent comprendre qu'une attaque DDoS ne vise pas seulement à rendre inopérant un site Web ou un autre service : ces attaques peuvent également servir à masquer l'utilisation de programmes malveillants perfectionnés pour voler des informations sensibles de l'entreprise. »

Conclusion

Bien que la perception qu'en ont les entreprises ne soit pas toujours conforme à la réalité, les cybermenaces ne sont bel et bien pas près de disparaître. Elles continuent d'évoluer pour s'adapter à l'évolution du paysage informatique au sein des entreprises, voire garder une longueur d'avance sur ces changements.

Les cybercriminels continueront toujours d'innover et il est important que leur conscience croissante des menaces actuelles ne rende pas les entreprises aveugles aux menaces appelées à émerger. Les entreprises doivent donc non seulement s'engager sur la voie de la formation continue, mais aussi faire de la sécurité une composante essentielle de leurs plans d'investissement en informatique.

Dès lors que vous investissez dans la virtualisation, migrez des ressources dans le cloud ou accordez plus d'importance au travail mobile, vous devez impérativement prendre en compte le fait que ces opportunités s'accompagnent de risques qui doivent être combattus.

Compte tenu de sa relation avec ces préoccupations stratégiques, la cybersécurité doit être intégrée aux décisions prises en plus haut lieu, et non plus être gérée après coup au lendemain des décisions prises au sommet de la hiérarchie. Ainsi, si le travail mobile est débattu en conseil d'administration, la protection nécessaire pour le rendre possible et le sécuriser doit également faire partie des sujets abordés. Ce n'est malheureusement pas le cas aujourd'hui.

Cette situation doit changer. En repensant notre façon d'envisager la sécurité et de l'intégrer aux budgets, nous pouvons nous assurer qu'elle demeure adéquate pour protéger un paysage informatique en évolution permanente.

L'équipe GReAT

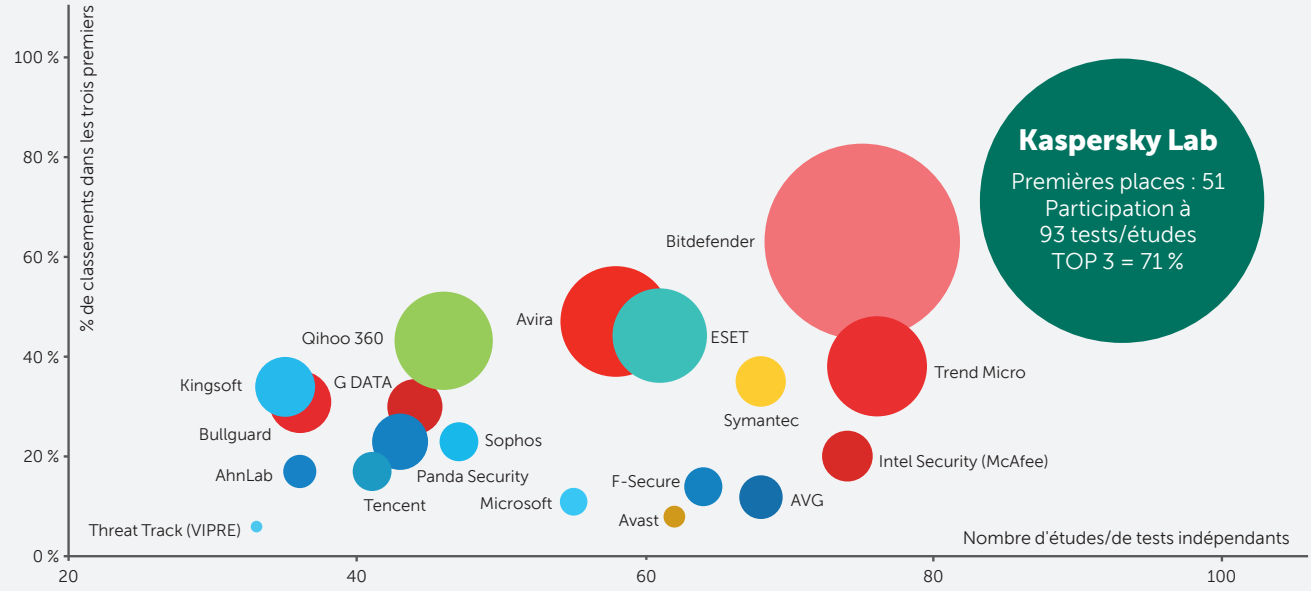
Les informations contenues dans ce rapport sont fournies par l'équipe Global Research and Analysis de Kaspersky Lab (GReAT). Depuis 2008, l'équipe GReAT ouvre la voie en matière d'informations, de recherche et d'innovation sur la protection contre les menaces, au sein de Kaspersky Lab et en externe. Le GReaT a été à l'avant-garde de l'analyse de certaines des menaces les plus sophistiquées au monde, y compris Stuxnet, Duqu, Flame, Red October, NetTraveler, Careto, Equation, Carbanak et Duqu 2.0.

Pourquoi Kaspersky Lab ?

Classé parmi les quatre plus grands spécialistes mondiaux de la sécurité, Kaspersky Lab est l'un des fournisseurs de solutions de sécurité informatique enregistrant la croissance la plus rapide au monde. Présents dans près de 200 pays et territoires à travers le monde, nous fournissons une protection à plus de 400 millions d'utilisateurs et plus de 270 000 entreprises clientes de toutes tailles, des petites et moyennes entreprises aux grandes organisations gouvernementales et commerciales.

Nos solutions de sécurité intégrées et avancées permettent aux entreprises de contrôler de manière inégalée l'utilisation des applications, du Web et des périphériques : vous définissez les règles et nos solutions vous aident à les gérer.
Kaspersky Endpoint Security for Business est spécifiquement conçue pour combattre et bloquer les menaces persistantes sophistiquées d'aujourd'hui. Déployée parallèlement à Kaspersky Security Center, cette solution donne aux équipes de sécurité la visibilité et le contrôle dont elles ont besoin, quelles que soient les menaces auxquelles elles font face.

En 2014, les produits Kaspersky Lab ont fait l'objet de 93 études et tests indépendants. Nos produits ont figuré 51 fois en première position et 66 fois parmi les trois premiers.*



** Remarques : d'après le résultat synthétisé d'un test indépendant réalisé en 2014 pour les produits d'entreprise, grand public et mobiles.*

La synthèse comprend les tests effectués par les laboratoires et les magazines indépendants suivants : Laboratoires de test : AV-Comparatives, AV-Test, Dennis Technology Labs, MRG Effitas, NSS Labs, PC Security Labs, VirusBulletin. La taille de la bulle correspond au nombre de premières places.

NOTRE EXPERTISE AU SERVICE DE VOTRE ENTREPRISE

Dans un contexte où les menaces sont de plus en plus sophistiquées et complexes, une plateforme de sécurité multi-niveaux protégeant contre les menaces connues, inconnues et avancées devient indispensable.

Rendez-vous sur **http://www.kaspersky.fr/entreprise-securite-it/** pour en savoir plus sur l'expertise unique de Kaspersky Lab et sur ses solutions de sécurité destinées aux entreprises.

EN SAVOIR PLUS

RETROUVEZ-NOUS SUR LES RÉSEAUX SOCIAUX

#EnterpriseSec

Visionnez nos vidéos sur YouTube

Rejoignez nos fans sur Facebook

Suivez-nous sur Twitter

Retrouvez-nous sur LinkedIn

Retrouvez-nous sur viruslist

Découvrez notre blog https://business.kaspersky.com

Rejoignez-nous sur Threatpost

Retrouvez-nous sur Securelist

À PROPOS DE KASPERSKY LAB

Kaspersky Lab est l'une des entreprises de cybersécurité connaissant la croissance la plus rapide au monde. C'est aussi la plus grande société privée du secteur. Elle fait partie des quatre principaux éditeurs mondiaux de solutions de sécurité informatique (IDC, 2014). Depuis 1997, Kaspersky Lab a été pionnière en matière de cybersécurité. Elle offre des solutions de sécurité informatiques efficaces et une surveillance des menaces pour les grandes entreprises, les PME et les consommateurs. Kaspersky Lab est une société internationale et est actuellement présente dans près de 200 pays et territoires à travers le monde, où elle apporte une protection à plus de 400 millions d'utilisateurs.

http://www.kaspersky.fr/entreprise-securite-it/
#EnterpriseSec