67 % DES ORGANISATIONS EN FRANCE ONT SUBI AU MOINS UNE VIOLATION DE DONNÉES SUR LES 12 DERNIERS MOIS

Une enquête du Ponemon Institute révèle que seules 9% des organisations interrogées disposent d'une stratégie homogène de chiffrement sur l'ensemble de leur périmètre.

PARIS et Menlo Park, Californie / le 9 septembre 2009 – PGP Corporation, un leader mondial de la protection des données d'entreprise, annonce les résultats de sa toute première enquête menée par le Ponemon Institute, qui vise à identifier les tendances des organisations françaises en matière de protection de leurs données confidentielles. Le rapport *Enquête annuelle 2009 : tendances en matière de chiffrement des données d'entreprise en France* s'est penché sur un panel de 414 professionnels de la sécurité informatique en France, issus d'organisations du Service Public et d'entreprises. Les résultats montrent que 67 % des organisations françaises ont subi au moins une violation de données au cours de l'année passée, tandis que 18% d'entre elles avouent plus de 5 incidents de sécurité de ce type. 92 % de ces violations de données n'ont jamais été rendus publics, puisque, à ce jour, aucune réglementation ne l'impose. En dépit de ce volume impressionnant de violations de sécurité, 71% des personnes interrogées considèrent la protection de leurs données comme une brique « importante » ou « très importante » de leur stratégie de gestion des risques. La priorité est à la protection des données stockées et mobiles.

« Il est très encourageant de constater que 71 % des personnes interrogées font de la protection des données un axe essentiel de leur stratégie globale de gestion des risques », observe Larry Ponemon, Président et Fondateur du Ponemon Institute. « Pour autant, les organisations françaises restent trop peu nombreuses à mettre en œuvre une stratégie globale de chiffrement basée sur une plateforme, et de nombreuses améliorations sont encore à venir sur le sujet. L'objectif pour 2010 devra faire de la sécurité des données un enjeu stratégique sur l'ensemble de l'entreprise. »

Voici une synthèse des principaux résultats de l'enquête 2009 sur les tendances en matière de chiffrement en France :

- **Seules 9% des organisations disposent d'une stratégie globale de chiffrement, appliquée de manière homogène sur l'ensemble de leur périmètre.** 45% d'entre elles n'ont aucune initiative ou stratégie sur le sujet. Les 46% restants modulent leur projet de chiffrement selon le type d'application ou de données, ou utilisent le chiffrement que pour certaines informations confidentielles (numéros de sécurité sociale ou numéros de carte de paiement par exemple).
- **Les principaux moteurs du chiffrement : la mise en conformité réglementaire en matière de sécurité des données (pour 65 % des organisations interrogées), et la volonté d'éviter l'impact d'une violation de données sur son image de marque et sur sa réputation (43 %).** Les recommandations de la CNIL et de la loi française en matière de confidentialité constituent les deux principales réglementations qui incitent les organisations à opter pour le chiffrement (à hauteur de 66% et de 62% respectivement). L'impact des lois internationales comme Sarbanes Oxley est mineur (4 %).
- **11% des organisations ont opté pour une plateforme pour gérer le chiffrement sur l'ensemble de leur périmètre et leurs applications.** 82% de ces organisations estiment qu'une plateforme de chiffrement dope l'efficacité de leur politique de sécurité informatique. La réduction des coûts d'exploitation, une application homogène des règles sur l'ensemble des applications, et l'intégration avec des solutions de chiffrement de fournisseurs tiers, comptent parmi les avantages les plus appréciés.
- **56 % des répondants utilisent partiellement le chiffrement tandis que les 44% restants sont en train d'introduire cette technologie**. Le chiffrement est essentiellement utilisé pour protéger les données dans les bases de données, ainsi qu'au niveau des VPN et des serveurs de fichiers. Le chiffrement des systèmes mainframe et des clés USB est le moins courant.
- **71% des organisations ont initié ou ont entièrement déployé des systèmes d'archivage des données et de recherche de preuves (e-discovery).** Ce chiffre ressort légèrement plus bas (70 %) en matière de technologie de prévention et de détection des fuites de données. Plus de la moitié des personnes interrogées (58 %) ont initié ou ont déployé une technologie de monitoring des postes client et serveurs (endpoint).
- **67 % des personnes interrogées reconnaissent avoir subi au moins une violation de données au cours des 12 derniers mois.** Parmi les entreprises qui ont connu plus de 2 violations, aucune d'entre elles ne disposait d'une stratégie d'entreprise de chiffrement.

- **Une majorité des personnes interrogées (58 %) considèrent comme « important » ou « très important » la possibilité de n'avoir à déployer qu'une seule plateforme de chiffrement, puis d'y adosser de nouvelles applications de chiffrement à la demande.** Une gestion automatique des clés de chiffrement (55%) et la possibilité de mettre en œuvre des règles de chiffrement sur l'ensemble de leur entreprise sont des avantages considérés comme importants.

- **Les solutions de chiffrement sont devenues une priorité pour 39% des personnes interrogées.** 29% d'entre elles indiquent également que les solutions de gestion des clés de chiffrement figurent parmi les initiatives de sécurité inscrites au budget actuel, et représentent un peu plus de 21% du budget dédié au chiffrement.
- **45 % des personnes interrogées considèrent que la perte ou le détournement de données confidentielles ou sensibles est une menace de sécurité majeure dans les 12 à 24 mois à venir.** Pour autant, 68% des organisations ne chiffrent pas encore les données présentes sur les équipements mobiles de types smartphones ou assistants personnels, tandis que seules 4 % chiffrent les données sur clés USB. 47 % de ces organisations ne sont pas sûres ou n'ont pas confiance en leur capacité à protéger les données confidentielles en environnement mobile.

« Les chiffres du Ponemon Institute démontrent que la conformité réglementaire et la crainte d'une atteinte à son image de marque incitent les organisations françaises à donner la priorité à la protection des données », constate Phillip Dunkelberger, Président et CEO de PGP Corporation. « Les solutions de chiffrement des données confidentielles, lorsque mises en œuvre de manière cohérente et homogène sur l'ensemble de l'entreprise, sont parfaitement capables de protéger les données stockées, mobiles ou en cours d'utilisation ».

Pour toute information supplémentaire ou pour recevoir le rapport de cette enquête, rendez-vous sur www.encryptionreports.com

À propos du Ponemon Institute

Le Ponemon Institute© a pour ambition de promouvoir l'éthique en matière d'information et les meilleures pratiques de gestion de la confidentialité au sein des entreprises et des administrations. L'Institut mène ainsi des études indépendantes, sensibilise les acteurs des secteurs publics et privés, et évalue les pratiques de confidentialité et de sécurité des données d'organisations représentatives de nombreux secteurs d'activité.

À propos de PGP Corporation

PGP Corporation est un leader mondial du chiffrement des données et des emails dans le cadre de la protection des données d'entreprise. La plateforme de chiffrement PGP est basée sur une gestion des clés et sur une infrastructure de règles unifiées et offre la plus large gamme d'applications intégrées et dédiées à la sécurité des données d'entreprise. Les solutions PGP® répondent aux besoins actuels des entreprises, mais anticipent également les besoins futurs liés à l'évolution du cadre de sécurité qui s'applique aux emails, ordinateurs portables, postes de travail, messageries instantanées, stockage réseau, transferts de fichiers, processus automatisés et autres sauvegardes.

Les solutions de PGP sont utilisées par plus de 100 000 organisations (entreprises et instances du service public) dans le monde, dont 95% des entreprises du palmarès Fortune® 100, 75 % de celles inscrites au Fortune® Global 100, ainsi que 87 % des entreprises du DAX allemand et 51 % du FTSE 100 britannique. Cette réussite confère aux solutions normalisées de PGP une réputation mondiale d'innovation et de confiance. PGP Corporation assure la confidentialité des données, sécurise les données clients, favorise la conformité au cadre réglementaire en vigueur, et, au final, pérennise l'image de marque et la réputation des entreprises. Rendez-vous sur www.pgp.com pour toute information supplémentaire.

Sphère de sécurité – Déclarations prévisionnelles

Certaines déclarations abordées dans ce communiqué de presse constituent des déclarations prévisionnelles et comptent notamment les déclarations sur la disponibilité, les plans, le déploiement, le développement, les fonctionnalités attendues et les avantages attendus des produits PGP qui utilisent les technologies de PGP. Toute référence relative aux améliorations de fonctionnalités, à la prise en charge de plateformes ou à de nouvelles fonctionnalités est susceptible d'être modifiée sur décision unilatérale de PGP Corporation. Toute description future des technologies et produits de PGP ne sera concrétisée que si PGP décide de les développer et si PGP Corporation décide de les commercialiser. Ces dernières impliquent des risques et des incertitudes pouvant se traduire par des résultats réels très différents de ceux indiqués dans les déclarations prévisionnelles. Liste non exhaustive de ces risques et incertitudes : difficultés technologiques et erreurs logicielles non prévisibles et liées à la finalisation et à la commercialisation des produits de PGP, changements technologiques, réglementaires ou dans les normes de sécurité, de chiffrement et d'authentification qui pourraient rendre les produits de PGP moins compétitifs ou requérir de nouvelles fonctionnalités pour les produits, les ralentissements dans l'adoption par les entreprises de logiciels de chiffrement, de sécurité email, des technologies Internet notamment.