

COMMUNIQUE DE PRESSE

UTILISATION DES APPLICATIONS WEB 2.0 EN ENTREPRISE : LES SALARIES FRANÇAIS IGNORENT LES CONSIGNES DE SECURITE

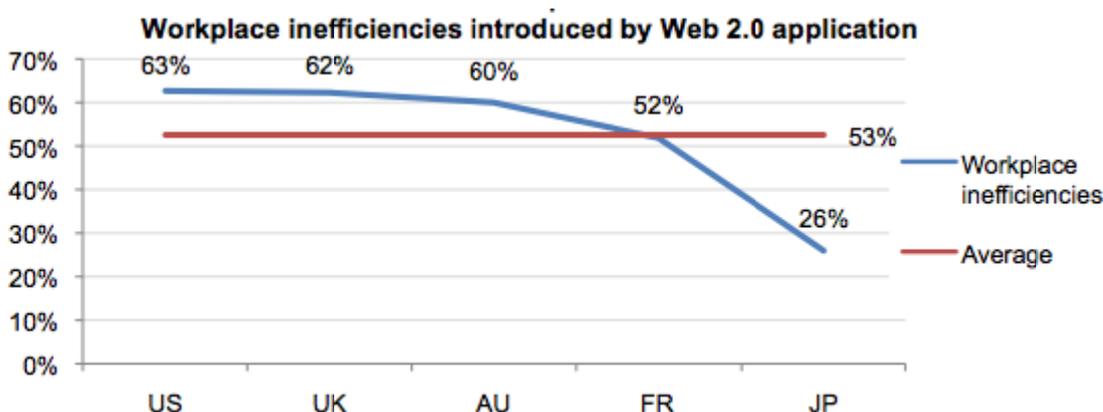
Selon une étude menée conjointement par Check Point et le Ponemon Institute, les applications Web 2.0 continuent de poser un défi pour la sécurité d'entreprise. Cette étude révèle un besoin de sensibilisation des utilisateurs et un contrôle renforcé des applications en entreprise.



PARIS –8 septembre 2010– [Check Point® Software](#) (Nasdaq: CHKP), leader mondial de la sécurité Internet et le [Ponemon Institute](#), un cabinet spécialisé dans le domaine de la gestion et la protection des données, publie les résultats d'une étude internationale sur *la Sécurité sur le Web 2.0* en milieu professionnel. Selon cette étude, les réseaux sociaux et les applications Web 2.0 constituent une menace de sécurité pour l'entreprise selon 74% des organisations françaises interrogées. Les administrateurs de la sécurité

informatique citent en premier lieu les virus, la baisse de la productivité, la perte de données et les logiciels malveillants comme les principaux risques liés à l'utilisation du Web 2.0 en entreprise. Pas moins de 81% d'entre eux envisagent de déployer une solution ciblée au cours des cinq prochaines années.

Selon l'enquête, menée en France auprès de 400 administrateurs de la sécurité informatique, la majorité des personnes interrogées considère que c'est au personnel des ressources humaines, des services informatiques et aux administrateurs de la sécurité qu'il revient de gérer les risques de sécurité liés à l'utilisation des applications Web 2.0 en entreprise. 52% des répondants considèrent que les utilisateurs ne tiennent pas ou peu compte des risques informatiques lors de leurs échanges professionnels de tous les jours, lorsqu'ils naviguent sur le Web en entreprise, téléchargent des applications, lorsqu'ils ouvrent des liens ou s'aventurent sur des sites de réseaux sociaux. Bien qu'ils offrent une pléthore d'avantages pour les entreprises, les applications du Web 2.0, et les sites tels que Facebook, Twitter, YouTube, les sites de partage de fichiers (peer-to-peer) et autres, constituent néanmoins un vecteur d'attaques pour le moins redoutable pour les entreprises, et jouissent d'une popularité croissante auprès des pirates.



Autres résultats de l'enquête:

- **Une préoccupation secondaire** - Malgré la forte montée des menaces sur le Web 2.0, les répondants en France se montrent relativement moins préoccupés par la sécurité du Web 2.0, que leurs homologues aux États-Unis, Royaume-Uni, au Japon ou Australie. Seulement 25% des professionnels français interrogés considèrent la sécurité sur le Web 2.0 comme une forte priorité, contre 65% aux États-Unis, 69% au Japon, et 43% en Australie et Grande-Bretagne.
- **Une responsabilité limitée de l'utilisateur** - La majorité des personnes sondées en France estime qu'il revient avant tout aux services du personnel, aux agents informatiques (DSI) et aux responsables de la sécurité (DSSI) de contrôler les risques du Web 2.0 sur la sécurité dans l'entreprise, et non pas aux employés qui les utilisent, ni aux services juridiques de l'entreprise. Leurs homologues aux États-Unis, en Australie et Grande-Bretagne pour la plupart considèrent que ce sont au contraire les employés qui devraient être tenus responsables de préserver la sécurité informatique de leur entreprise lors de leur utilisation du Web 2.0.
- **Les principaux ennemis** – les virus informatiques, la baisse de la productivité au travail et les logiciels malveillants sont cités comme les principales préoccupations relatives à l'utilisation des applications Web 2.0 dans les entreprises françaises. Parmi les autres problèmes cités figurent aussi la perte de données, la saturation de la bande passante, les botnets et les injections SQL.
- **Un manque global de conscience sécuritaire** – Près de 52% des personnes interrogées aux États-Unis considère que leurs employés prennent rarement ou jamais en compte les questions de sécurité lors de l'utilisation de réseaux sociaux et applications Web 2.0 dans leurs communications professionnelles. Ce chiffre atteint 49% au Royaume-Uni et 48% en Australie.

« Cette enquête révèle un certain décalage dans les organisations françaises entre d'une part le personnel d'entreprise, qui souhaite continuer de profiter des outils Web 2.0, et d'autre part les administrateurs informatiques chargés de garantir la sécurité du réseau et la bonne application des politiques de sécurité » déclare David Darmon directeur général France de Check Point Software. *« Souvent les administrateurs manquent de visibilité et n'ont pas les moyens de gérer la sécurité des multiples applications du Web 2.0 déployées sur le réseau. Or mettre en œuvre une solution de sécurité flexible capable d'administrer les outils du Web 2.0 exige davantage de visibilité, ainsi qu'une plus large sensibilisation des utilisateurs et un contrôle granulaire des applications. Il s'agit à la fois d'un défi technologique et d'une question d'éducation des employés. »*

Check Point a longtemps protégé les entreprises contre les menaces émergentes. Aujourd'hui, Check Point lance sa nouvelle lame logicielle [Contrôle des applications](#). Basée sur son architecture software blade, cette solution permet aux sociétés de sécuriser et gérer l'utilisation de milliers d'applications Web 2.0 dans l'entreprise. A travers sa technologie novatrice UserCheck, les employés participent au processus de prise de décision, permettant aux administrateurs informatiques d'adapter l'utilisation des applications en fonction de leurs besoins commerciaux spécifiques. La nouvelle lame tire également parti de [Check Point AppWiki](#), la plus grande base de données au monde de classification des applications, qui permet d'examiner plus de 50.000 widgets Web 2.0 et plus de 4.500 applications Internet. Pour de plus amples informations: <http://www.checkpoint.com/products/softwareblades/application-control.html>.

Cette étude sur la sécurité du Web 2.0 en milieu de travail a été réalisée indépendamment par le Ponemon Institute en avril 2010, auprès 400 administrateurs en France et plus de 2.100

administrateurs de la sécurité informatique au total, situés aux États-Unis, Royaume-Uni, France, Japon et Australie. L'échantillon de l'enquête représente un large éventail d'organisations de toutes tailles - des petites et moyennes entreprises aux grandes entreprises - et tous secteurs économiques, y compris du secteur financier, industriel, gouvernemental, de la grande distribution, de la santé et de l'éducation. Pour consulter le rapport complet en anglais, veuillez vous http://www.checkpoint.com/products/downloads/whitepapers/ponemon_white_paper.pdf.

« Les menaces informatiques provenant des applications Web 2.0 s'intensifient tant dans leur fréquence que dans leur complexité. Il est important que les entreprises françaises reconnaissent le problème pour en faire l'une de leurs priorités, à l'instar de leurs homologues américains ou britanniques. Seuls une sensibilisation accrue des utilisateurs et un meilleur contrôle des applications réalisé par le biais d'une solution performante, permettra aux employés de continuer à bénéficier des outils du Web 2.0 sans pour autant compromettre la sécurité de leur entreprise. Aujourd'hui Check Point offre aux entreprises une approche pratique pour le contrôle des applications qui permet aux employés de continuer à utiliser les outils du Web 2.0, sans pour autant compromettre la sécurité de leur entreprise » conclut David Darmon.

A propos de l'Institut Ponemon

Le Ponemon Institute© vise à promouvoir les meilleures pratiques en matière d'information et de gestion de la confidentialité. Dans cette optique, l'Institut mène des études indépendantes, sensibilise les différents acteurs des secteurs public et privés et audite les pratiques de protection et de confidentialité des données pour des organisations situées dans divers secteurs d'activité, privées ou publiques.

À propos de Check Point Software Technologies Ltd.

Check Point Software Technologies Ltd. (www.checkpoint.com) est le leader de la sécurité Internet et est le seul à proposer des solutions de sécurité totale pour les réseaux, les données, les postes de travail au travers d'une administration centralisée. Cette approche unique offre aux clients de Check Point une protection incomparable face aux différentes attaques, optimise les installations et réduit considérablement les coûts de possession. L'architecture dynamique « Software Blade » propose des solutions hautement sécurisées, modulables et simples qui peuvent être adaptées à tout type de besoins suivant les organisations ou l'environnement.

Check Point compte parmi ses clients les 100 sociétés figurant au classement des Fortune 100 ainsi que plusieurs dizaines de milliers d'entreprises et d'organisations de toute taille.

De plus, les solutions ZoneAlarm protègent les PC de millions de particuliers contre les pirates, les logiciels espions et les vols de données.

©2010 Check Point Software Technologies Ltd.

###