

Check Point Software : Les menaces cachées sur la sécurité des réseaux de PME Internet

Posté par : JulieM

Publié le : 20/1/2014 13:30:00

Son rapport 2013 définit les priorités que doivent adopter les organisations du monde entier en matière de sécurité. **Check Point® Software Technologies Ltd**, le leader mondial de la sécurité Internet, publie son rapport sur la sécurité 2013 dans lequel il dévoile **les risques majeurs pour la sécurité des organisations à travers le monde.**

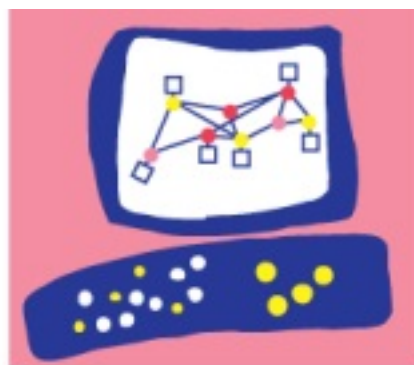
Dans ce nouveau rapport, Check Point analyse les principales menaces informatiques, les applications Web à risque qui compromettent la sécurité des réseaux et les pertes de données résultant de l'ignorance des employés. Plus important encore, ce rapport formule des recommandations quant aux mesures de protection à mettre en oeuvre contre ces menaces.

Au vu de la course poursuite observée en 2012 entre les pirates et les services informatiques, il est apparu clairement que bon nombre des menaces les plus sérieuses restaient méconnues des administrateurs réseau.

Ces menaces sont le fruit des stratégies en perpétuelle évolution mises au point par les cyber-criminels, mais naissent aussi des activités à risque menées en ligne par certains employés qui créent ainsi, sans le vouloir, des failles de sécurité sur le réseau de l'entreprise.

Afin de concevoir un plan de sécurité qui tient la route, les entreprises doivent d'abord prendre connaissance des activités qui sont opérées sur leur réseau et en comprendre les tenants et les aboutissants.

À partir d'une étude portant sur près de 900 entreprises, le rapport sur la sécurité 2013 de Check Point permet de découvrir ce qui se cache sur les réseaux d'entreprise et met en lumière les principales menaces auxquelles les organisations sont exposées au quotidien :



Check Point®
SOFTWARE TECHNOLOGIES LTD.

Menaces cachées pour la sécurité :

Depuis les crimeware jusqu'à la tendance « hacktiviste », les cyberattaques continueront d'évoluer cette année pour toucher les organisations de toute taille.

D'après les résultats de l'étude, 63 % des entreprises sont infectées par des bots et plus de la moitié sont prises pour cible au moins une fois par jour par un nouveau logiciel malveillant.

Le rapport dévoile une liste des principales menaces, y compris les botnets les plus dévastateurs, des lieux les plus touchés par les logiciels malveillants dans chaque pays, des principales failles de sécurité et vulnérabilités chez chaque éditeur de solutions et des cas d'injection SQL par pays d'origine, entre autres conclusions toujours plus surprenantes.

Applications Web 2.0 à risque :

L'essor des applications Web 2.0 a permis aux cyber-criminels de bénéficier d'un choix d'options sans précédent pour infiltrer les réseaux d'entreprise. D'après les résultats de l'étude, 91 % des entreprises utilisent des applications présentant des risques potentiels pour la sécurité.

Ces applications Web à risque sont détaillées dans le rapport, qui précise également la fréquence et le mode d'utilisation des anonymiseurs, des applications P2P, des applications de stockage et de partage de fichiers et des principaux réseaux sociaux à ces plateformes étant toutes susceptibles d'ouvrir une porte d'entrée donnant accès aux réseaux d'entreprise.

Incidents conduisant à la perte de données :

Il est plus facile que jamais d'accéder aux informations d'une entreprise et de les transférer, ce qui accroît le risque de perte ou de fuite de données. Plus de la moitié des entreprises à l'étude ont subi au moins un incident ayant pu causer une perte de données.

Le rapport expose les différents types de données sensibles faisant l'objet de pertes et de fuites, parmi lesquelles on retrouve les renseignements relatifs aux cartes de paiement et les informations médicales protégées par la loi HIPAA. Il permet également de mieux comprendre les secteurs les plus susceptibles d'être affectés.

« Dans le cadre de nos travaux de recherche, nous avons découvert de nombreuses vulnérabilités et menaces préoccupantes pesant sur la sécurité des réseaux qui ont échappé à la vigilance de la plupart des entreprises », déclare **Amnon Bar-Lev**, président de [Check Point Software Technologies](https://www.checkpoint.com).

« Les professionnels du secteur informatique bénéficient désormais d'une visibilité accrue leur permettant de finir plus efficacement un plan de sécurité visant à protéger leur entreprise du flux constant de nouvelles menaces à des botnets à la perte de données, en passant par les applications Web à risque telles que les anonymiseurs. »

« Le rapport sur la sécurité 2013 de Check Point est un vibrant appel à l'action. Il propose une analyse exclusive du paysage actuel de la cybercriminalité et des tendances qui se dessinent », déclare **Alberto Dosal**, président du conseil d'administration de Compuquip Technologies, l'un des plus grands prestataires de services informatiques entièrement intégrés du sud de la Floride.

« C'est un document complet et vraiment impressionnant, que tout dirigeant se doit absolument de lire. »

Leader de confiance dans le secteur de la sécurité, Check Point aide les entreprises de toute taille à mettre en place un plan de sécurité et une architecture répondant parfaitement à leurs besoins.

Son portefeuille de produits maintes fois primé lui permet d'instaurer un protocole de sécurité multicouche qui protège les entreprises contre tous les types de menace identifiés dans le rapport.

Les passerelles de sécurité Check Point exécutent les « software blades » Check Point (p. ex. IPS, contrôle des applications, filtre des URL, antivirus et anti-bot) afin de détecter et de contrer les nouvelles menaces. Le système Check Point ThreatCloud® alimente en temps réel la base des signatures de ces applications logicielles.

Par ailleurs, la passerelle Web sécurisée Check Point bloque l'accès aux sites Web infestés de logiciels malveillants, ainsi que l'utilisation des applications à haut risque comme les anonymiseurs. Enfin, la solution DLP Check Point aide les entreprises à protéger préventivement leurs données sensibles pour éviter toute perte ou fuite accidentelle.