



WatchGuard identifie le top 10 des menaces liées à la sécurité réseau des PME

Paris le 24 septembre 2008 - Watchguard Technologies, fournisseur global de solutions de sécurité réseau, a recherché et identifié les 10 principales menaces liées à la sécurité informatique des PME.

Contrairement aux grandes entreprises, les PME sont confrontées à de multiples menaces liées à leur sécurité informatique, et elles disposent souvent de ressources limitées pour protéger leurs actifs, données et informations clients.

« Les menaces liées à la sécurité informatique des PME sont aussi réelles que pour les grands comptes », déclare Eric Aarrestad, vice-président du marketing chez Watchguard Technologies. « La tragédie est que beaucoup de PME ne sont tout simplement pas informées que des appliances UTM (Unified Threat Management) peuvent lutter contre ces menaces. »

Les 10 principales menaces liées à la sécurité informatique identifiées par Watchguard :

- 1) **Des correctifs non téléchargés ouvrant la voie aux Exploits** – plus de 90 % des attaques automatisées visent à tirer partie des failles existantes. Bien que des correctifs soient publiés régulièrement, une majorité des PME omettent de mettre à jour leurs applications ou d'installer ces derniers au niveau de leurs systèmes les laissant vulnérables à des attaques qui peuvent être facilement stoppées.
- 2) **E-mail HTML à risque** – les attaques malveillantes ne se font désormais plus à travers l'envoi d'e-mails avec des pièces jointes piégées. Aujourd'hui les menaces sont cachées derrière les messages html sous forme de lien. Un mauvais clic peut vous conduire à l'installation et à l'exécution d'un programme malveillant (drive by download).
- 3) **Navigation internet imprudente** – aujourd'hui plus que jamais, logiciels malveillants, logiciels espions, keyloggers et spambots sont hébergés sur des sites à priori sans danger. Les employés qui s'aventurent sur ces sites d'apparence inoffensive peuvent inconsciemment exposer les réseaux de leur entreprise à de graves menaces.

- 4) **Navigateur vulnérable** – de nombreuses PME hébergent leur propre site Internet sans protection adéquate, laissant leurs réseaux professionnels exposés à des injections SQL et des attaques botnet.
- 5) **Perte des appareils mobiles** – chaque année, les données des PME sont compromises en raison de la perte d'ordinateurs portables, de mauvais rangement d'appareils mobiles ou de clés USB égarées. Bien que le cryptage des données et l'utilisation de mots de passe atténuent les risques de perte, nombreuses sont les PME qui négligent de sécuriser leurs appareils mobiles.
- 6) **Utilisation imprudente des serveurs publics** – une ruse commune aux pirates est de mettre à disposition un accès sans fil non sécurisé, intitulé "WiFi gratuit" et de simplement attendre qu'une personne vienne se connecter. Avec un « packet sniffer » activé, le pirate peut ainsi furtivement voir tout ce que l'employé voit, il est alors en mesure d'utiliser ces données à ses fins personnelles.
- 7) **Domicile non sécurisé** – dans de nombreuses PME, les employés emportent souvent leurs ordinateurs portables professionnels chez eux. Dans un environnement réseau au domicile non sécurisé, un ordinateur portable peut être gravement exposé à des virus, des attaques et à des logiciels malveillants.
- 8) **Des identifiants par défaut inchangés** – Les hackers publient et tiennent à jour une liste exhaustive des identifiants par défaut de presque tous les dispositifs réseau. Ils peuvent ainsi facilement prendre contrôle des ressources du réseau si les paramètres de configuration par défaut ne sont pas modifiés.
- 9) **Le manque d'un plan de restauration** – une des plus grandes menaces qui pèse sur les PME, c'est l'impact après un piratage, une intrusion ou un virus. Beaucoup de PME ne disposent pas de politique de réponse en cas de perte de données ou de plan de restauration après sinistre, laissant alors leur entreprise récupérer et redémarrer lentement.
- 10) **Initiés** - dans de nombreuses PME, les documents professionnels et données des clients sont souvent confiées à une seule personne. Sans aucune politique de contrôle ou de vérification régulière des accès aux systèmes réseaux et aux rapports automatisés, les pertes de données peuvent parfois s'étaler sur de longues périodes.

« Des réseaux sécurisés garantissent aux entreprises une liberté de productivité et d'efficacité », ajoute Carl Mazzanti, Directeur Général de eMazzanti Technologies, un fournisseur régional de services de sécurité administrés. "Les PME qui sont vigilantes et qui maintiennent un haut niveau de sécurité ont tendance à devenir des leaders dans leurs industries. »

Mots clés :

PME, réseau, configuration, appareils mobiles, serveur web, navigation internet, HTML, e-mail, correctifs, vulnérabilités, risques, sécurité, traitement des menaces, Watchguard.

A propos de WatchGuard

Depuis 1996, WatchGuard® Technologies, Inc. est leader technologique dans les appliances de sécurité réseau, en fournissant des solutions de sécurité fiables et faciles à gérer à des centaines de milliers d'entreprises dans le monde. La famille WatchGuard Firebox® X de solutions de gestion unifiée des menaces (UTM) fournit la meilleure combinaison de sécurité puissante, fiable et multicouche avec la plus grande facilité d'utilisation dans sa catégorie. Tous les produits WatchGuard sont couverts par le service WatchGuard LiveSecurity®, un programme innovant de support, de maintenance et de formation. WatchGuard est une entreprise privée ayant son siège à Seattle, Washington, et des établissements dans toute l'Amérique du Nord, en Europe, dans la région Asie et Pacifique et en Amérique Latine.

Pour de plus amples informations, consultez <http://www.WatchGuard.fr>

Contacts Presse Open2Europe :**Rémi Brossard**

Tel : +33 1 55 02 14 74

E-mail : r.brossard@open2europe.com

Siham Morchid

Tel : +33 1 55 02 11 02

E-mail: s.morchid@open2europe.com