bitdefender

LIVRE BLANC

Nouvelles menaces pour la sécurité des entreprises

Aujourd'hui plus que jamais, il est important que les entreprises se préoccupent de la sécurité de leurs réseaux. Le nombre, la diversité et la puissance des menaces pesant sur la sécurité des ordinateurs et des réseaux ont redoutablement augmenté, et les entreprises doivent préparer leur défense face à un environnement en perpétuelle mutation.

Les fournisseurs de sécurité classiques s'intéressent essentiellement à la protection des applications informatiques. Toutefois, même si cet aspect reste important, aujourd'hui les menaces les plus graves – et celles dont on constate l'émergence – ont pour cible les nouveaux modes de vie en ligne. Le développement impressionnant de la maitrise des outils informatiques et la disparition relative de la frontière entre usage privé et professionnel des ordinateurs et des réseaux, font que les entreprises sont contraintes de surveiller de près l'activité de leurs employés sur leur réseau et de vérifier que leur sécurité n'est pas mise en cause.

Menaces pour l'environnement de l'entreprise
Les appareils mobiles : dernière voie d'accès des attaques

En 2007, les logiciels malveillants sont devenus une des menaces majeures pour la sécurité des réseaux. Les flux de codes malveillants sont continuels et la seule tendance perceptible aujourd'hui est la création de variantes à partir de codes existants, incluant des capacités de dissimulation toujours améliorées, et qui sont utilisées pour des attaques ciblées. De nombreux cas d'attaques contre des entreprises (via l'emploi de fichiers MS Office infectés principalement, mais d'autres techniques ont également été utilisées) ont récemment été rapportés. A chaque fois, le logiciel malveillant avait été écrit pour une attaque spécifique, et ne s'était pas beaucoup propagé en dehors de la société visée au départ. Alors que les logiciels malveillants poursuivent leurs attaques surprises, les entreprises doivent rester sur leurs gardes, sachant que ces logiciels sont de plus en plus sophistiqués et frappent là où les entreprises pensent être protégées.

Les appareils mobiles sont devenus un sujet de préoccupation face aux attaques de logiciels malveillants. L'utilisation de la technologie smartphone a joué un rôle central dans la transition entre les ordinateurs multifonction semi-fixes et les appareils «portables» tenant dans la paume de la main. La nouvelle tendance, qui est de proposer des mobiles avec des navigateurs intégrés et un accès permanent à Internet a élargi au monde des mobiles et aux entreprises, auxquelles ils sont connectés, les problèmes de sécurité du Web. Les virus qui exploitent les vulnérabilités des navigateurs vont devenir courants. En même temps que les performances augmentent, la sécurité est souvent troquée au profit des fonctionnalités, donnant le champ libre à toute une catégorie de nouvelles attaques malicieuses. Comme ils le font sur les ordinateurs, les virus peuvent, sur des appareils mobiles, supprimer ou infecter des fichiers, envoyer des informations privées, favoriser des attaques extérieures et/ou vider la batterie.

La meilleure défense des entreprises contre les logiciels malveillants
Il vaut mieux prévenir que guérir

Le vieil adage dit que «Il vaut mieux prévenir que guérir». Ce qui reste vrai pour les entreprises, même si la prévention dans ce cas est concrétisée par des politiques de sécurité. Des politiques de sécurité puissantes associées à des antivirus pour mobiles (si nécessaire) devraient diminuer la vulnérabilité des réseaux des entreprises. Les entreprises doivent admettre la nécessité urgente de protéger les appareils mobiles de leurs employés contre les attaques de codes malveillants qui peuvent mettre en péril la sécurité de leur réseau. Cette menace est réelle et devrait inciter les entreprises à envisager de déployer des solutions de sécurité dont la capacité à détecter de nouveaux codes malveillants et inconnus a été démontrée.

Autres menaces dans l'univers des entreprises - Et comment s'en prémunir

Le spyware reste un souci croissant pour les entreprises. A la lumière de la législation sur la protection des données récemment adoptée en Europe et aux Etats-Unis, le danger pour les entreprises, en termes de responsabilité pour le vol ou la perte de données va demeurer élevé.

Les différentes variantes de «Storm Worm» constituent la grande menace pour le début de 2008, tandis que la famille de trojans Zlob continue de croître et pourrait devenir une des menaces majeures l'an prochain. D'autres chevaux de Troie, qui créent des réseaux d'ordinateurs infectés et les utilisent pour propager des virus, du spam ou pour entreprendre des attaques de déni de service, pourraient également faire leur apparition. Pour les entreprises, le pare-feu reste le pilier principal de la sécurité du réseau contre les menaces automatisées, comme les vers et les botnets, s'il est associé à une solide protection antivirus à la fois au niveau du serveur et du client.

Les virus « mass mailer » étaient encore fréquents pendant la première moitié de 2007, mais d'autres catégories de menaces se révèlent, bien que le courrier électronique reste le moyen de prédilection pour d'autres types d'attaques. Le Adware voit son utilisation augmenter, car il comporte pour ses auteurs moins de danger juridique.

Le partage de fichiers P2P étant un usage déjà répandu, le nombre, la diversité et l'impact des infecteurs de fichiers sont destinés à augmenter au cours de l'année prochaine. Cependant, désactiver ou limiter le trafic P2P et les autres méthodes de partage de fichiers peut entraîner des coûts de productivité. Il est hautement recommandé d'installer des antivirus sur chaque ordinateur partageant des fichiers (qu'il s'agisse d'un simple ordinateur ou d'un serveur).

Le spam évolue et se diversifie, dans le but d'éviter les filtres en se modifiant en permanence et en masquant à la fois son contenu et son objectif. La quantité de spam sous forme de documents attachés, qui a eu tendance à diminuer au cours des derniers mois de 2007, augmente et pourrait de nouveau poser des problèmes en 2008. Dans la mesure où les pertes de productivité dues au spam ne sont pas négligeables, les PME devraient penser à déployer des filtres antispam à la fois au niveau du serveur et du poste client.

Le phishing (sur le Web comme par e-mail) est probablement la pire menace actuelle, et le restera l'an prochain. C'est aussi l'une des menaces les plus dangereuses parce que ses victimes subissent des pertes directes (comptes en banque «nettoyés» en quelques heures ou quelques jours). Le type le plus courant de spam de type phishing consiste à menacer de fermeture le compte visé par l'opération. Une variante répandue est de demander au client d'entrer les données de son compte pour «mettre à jour l'application de sécurité bancaire». Les modèles utilisés pour créer ces e-mails sont en général de très belle apparence et très semblables aux formulaires utilisés sur le Web par les banques cibles, bien que des erreurs d'orthographe et des adresses Web différentes des véritables banques subsistent dans beaucoup de cas.

Le spam phishing restera important l'an prochain (en termes de volume et de préjudice), avec les «améliorations» auxquelles on peut s'attendre en terme de techniques utilisées, à la fois pour déjouer les filtres antispam, et pour l'usage factice des authentifications SSL par des sites Web de phishing visant à se donner l'air crédible dans le navigateur de la victime. On s'attend également à ce que le nombre de banques ciblées augmente significativement. L'antiphishing est en phase de devenir une caractéristique incontournable pour n'importe quel logiciel de sécurité sur postes de travail.

Confrontées à un volume toujours plus important de menaces nouvelles ou existantes, les entreprises doivent envisager d'adopter des solutions de sécurité pouvant être déployées et administrées de manière centralisée, et être intégrées facilement au système de sécurité existant avec un minimum de frais. Les sociétés ne peuvent désormais plus compter sur simple la sécurité du réseau pour être effectivement en sécurité. Les menaces sont plus sophistiquées et la sécurité d'une société doit le devenir aussi.

Les entreprises ont besoin d'une solution de sécurité qui évalue la nature de l'activité des utilisateurs et les moyens utilisés pour les mettre en oeuvre, afin de déterminer proactivement où les menaces sont susceptibles de surgir et assurer une sécurité réseau totale.

Bogdan Dumitru – Responsable Technologique

A propos de BitDefender

Les technologies antivirus BitDefender protègent aujourd'hui plusieurs dizaines de millions d'utilisateurs dans plus de 180 pays, directement ou via leur intégration dans des applications tierces (IBM Internet Security System, GFI Mail Server, IPSwitch, Software602, etc.). Les moteurs de détection BitDefender sont certifiés par les organismes indépendants ICSA Labs, Checkmark, CheckVir, AV-Test, AV-Comparatives et Virus Bulletin. BitDefender a par ailleurs reçu le prix de l'innovation technologique décerné par la Commission Européenne (www.ist-prize.org). Les solutions Linux sont certifiées « RedHat Ready », « Ready for Suse Linux Enterprise Server », Ubuntu Software Partner et Mandriva. Les solutions BitDefender sont rééditées en exclusivité par Editions Profil sur les marchés francophones.

D'autres informations sont disponibles sur le www.bitdefender.fr

bitdefender

ÉDITIONS PROFIL
49, rue de la Vanne - 92120 Montrouge
Tél. (+33) 1 47 35 72 73
Fax (+33) 1 47 35 07 09
E-mail: bitdefender@editions-profil.eu
www.editions-profil.eu