bitdefender

LIVRE BLANC

Sécurité proactive - Armure pour la défense du système informatique des entreprises

Pourquoi lire ce livre blanc

Se défendre contre le nombre impressionnant des risques actuels peut constituer un gouffre ; en particulier pour les sociétés émergentes ou en pleine croissance, qui ont à faire face exactement aux mêmes menaces que les organisations plus développées, mais sans disposer des mêmes ressources informatiques.

Ce livre blanc évalue le terrain des risques actuels et montre en quoi s'appuyer sur une solution de sécurité intégrée peut apporter aux entreprises une protection plus efficace qu'une accumulation de solutions isolées, et pour un coût moindre.

L'évolution des logiciels malveillants

La sécurisation des réseaux constitue aujourd'hui un défi d'une ampleur inégalée. L'industrie du logiciel malveillant est devenue un commerce et les auteurs de codes malveillants ne sont désormais plus des gamins malicieux se livrant au cyber-vandalisme au petit bonheur la chance, mais plutôt des criminels organisés agissant dans le but de s'approprier de l'argent, des informations personnelles et confidentielles, voire les deux. Cette motivation prédatrice a eu pour conséquence un accroissement de la sophistication et de la fréquence des attaques et à la création de types de logiciels contre lesquels la lutte est devenue beaucoup plus difficile qu'elle ne l'était contre les virus d'autrefois écrits par des gamins. Les entreprises ont donc à faire face à des attaques plus élaborées, mais aussi à lutter à la fois contre des problèmes récurrents, comme le spam, et des risques plus récents, comme l'usage détourné d'Internet par leur personnel ou les manquements à la politique de l'entreprise.

L'expansion continuelle des risques entraîne le développement parallèle des besoins en ressources informatiques. Les grands voyageurs armés des plus récents appareils mobiles, cadres supérieurs et commerciaux portables sur les genoux, tous réclament un accès où qu'ils se trouvent, 24h/24 et 7j/7, à condition que cet accès leur ouvre de nouveaux points d'accès au réseau, lesquels contournent le traditionnel périmètre de sécurité. En outre les appareils portables, qui ne sont pas protégés ou le sont insuffisamment, peuvent constituer un danger pour le réseau de l'entreprise, menaçant à la fois l'intégrité des données et la poursuite de l'activité. En conséquence, la sécurité des postes de travail est devenue aussi indispensable que le périmètre de sécurité – mais garantir que les postes mobiles et fréquemment déconnectés sont sécurisés peut être hasardeux.

Panorama du risque aujourd'hui

Aujourd'hui, les entreprises doivent se protéger contre une quantité de menaces de plus en plus sophistiquées et au développement de plus en plus rapide, d'origine externe aussi bien qu'interne.

- **Omniprésence du World Wide Web.** Le Web est devenu le meilleur vecteur de menaces et se trouve en tête de la liste du SANS Institute des «Top dix des menaces pour la cybersécurité en 2008[1]. La vulnérabilité de nombreux navigateurs et plug-ins en font des cibles faciles pour les attaquants. Les attaques de sites Web sont elles aussi devenues plus complexes qu'auparavant et tentent maintenant d'exploiter simultanément des vulnérabilités diverses en déployant des mécanismes sophistiqués de dissimulation de leur charge malveillante face à la vigilance des produits de sécurité. En outre, ce ne sont pas seulement les sites appartenant au côté noir du Web qui présentent un risque, les sites Web légitimes sont fréquemment piratés et configurés pour transmettre du code hostile. Ce qui est particulièrement problématique dans la mesure où les utilisateurs appliquent des paramètres de sécurité différents aux sites Web considérés comme sûrs, ou sont simplement moins vigilants quand ils les visitent.

- **Prolifération des logiciels malveillants.** Les logiciels malveillants ont proliféré de façon endémique, avec plus de 5 millions de nouvelles souches ou variantes identifiées au cours de l'année 2007[2] - soit 4 millions de plus qu'au cours de l'année 2006. De plus, les virus destructifs ont perdu leur rang de numéro 1 au profit d'autres formes de logiciels malveillants plus furtifs et non destructeurs qui facilitent les objectifs crapuleux de vol d'argent et de données.

- **Augmentation du phishing.** Les attaques de type phishing deviennent de plus en plus courantes. Selon Gartner, 3,6 millions de personnes se sont fait escroquer 3 milliards de dollars au total au cours des 12 mois précédant août 2007[3]. Les consommateurs ne sont pas les seules cibles du phishing, les organisations subissent également des attaques de plus en plus fréquentes. Dans les attaques précisément ciblées ("spear phishing" - pêche au harpon), une information disponible est utilisée pour créer des messages électroniques d'apparence tout à fait plausible mais qui véhiculent une charge malveillante. En 2006, le réseau du Département d'Etat américain a été mis en péril par un code malveillant contenu dans un document attaché à un e-mail[4] de type pêche au harpon.

- **Perte de productivité et de ressources réseau.** Le spam est devenu une pandémie qui a coûté aux entreprises 100 milliards de dollars en 2007[5]. Au départ, le spam était utilisé en tant qu'outil commercial par quelques voyous à la petite semaine ; aujourd'hui, il est utilisé par des malfaiteurs organisés pour commettre des escroqueries pump-and-dump[6] leur assurant un bénéfice net atteignant des millions de dollars.

- **Brèche dans le périmètre réseau.** Les portables et les matériels informatiques mobiles sont devenus un véritable casse-tête pour les départements de ressources informatiques et classés comme un problème de sécurité majeur par les participants à la conférence InfoSecurity Europe 2007[7]. Faire respecter la politique de sécurité sur les appareils mobiles peut se révéler difficile et il en résulte que de tels appareils peuvent être insuffisamment sûrs – ce qui peut en faire les vecteurs de codes malveillants vers le réseau de l'entreprise d'une façon qui contourne complètement le traditionnel périmètre de sécurité.

- **La menace intérieure.** L'abus d'Internet par les personnels est devenu un problème considérable pour beaucoup d'entreprises. En Grande Bretagne, il a été estimé que la perte de productivité due à l'utilisation par les personnels des sites de réseaux sociaux, comme Facebook, pendant leurs heures de travail représente pour les entreprises un coût évalué à 6,5 milliards de livres[8] –soit un peu moins de 13 milliards de dollars américains- et que les connexions à de tels sites consomme environ 20 % de leur bande passante. En ajoutant à cela le temps passé sur des sites comme eBay et à la navigation en général, les coûts sont plus importants encore. Mais le fait est que les sites de réseaux sociaux ont effectivement une utilité et qu'en ce sens une interdiction générale ne peut en aucun cas être la solution.

En même temps que les attaques deviennent de plus en plus fréquentes et sophistiquées, elles deviennent aussi de plus en plus interconnectées. Les informations envoyées à des sites de réseaux sociaux sont récoltées pour être utilisées dans des campagnes de pêche au harpon > le code malveillant transmis par des emails de ce type piège des ordinateurs dans des botnets[9] (réseaux d'ordinateurs atteints contrôlés à distance et utilisés à des fins criminelles à l'insu ou sans le consentement de leurs propriétaires) > les botnets sont utilisés pour envoyer du spam qui contient une charge malveillante ou des liens vers des sites Web malveillants > d'autres ordinateurs sont infectés, piégés dans des botnets puis utilisés pour envoyer du spam pump-and-dump, lancer des attaques de type déni de service[10], expédier des emails de phishing et distribuer encore plus de codes malveillants.

Le véritable problème pour les entreprises aujourd'hui n'est pas tant de savoir comment se défendre contre une grande quantité de menaces diverses – il existe des produits qui répondent à chaque souci de sécurité - mais de savoir comment s'en défendre efficacement en termes de coût.

Le problème des solutions isolées

Les produits qui répondent à un aspect isolé de la sécurité informatique, comme la détection d'intrusions et les systèmes de protection (IDS et IPS), les produits antivirus, les filtres Web et anti-spam et une pléthore d'autres produits similaires qui assurent des fonctions importantes – mais peuvent créer une infrastructure de sécurité dont le coût peut être très élevé. Chaque solution isolée est une application supplémentaire, qui doit être installée, configurée, mise à jour et maintenue ; chacune signifie une relation supplémentaire à gérer avec un distributeur ; chacune ajoute un niveau de complication supplémentaire qui multiplie les interventions ; et chacune un logiciel supplémentaire auquel le personnel informatique devra être formé pour l'utiliser. En outre, dans la mesure où les solutions isolées conduisent à une architecture complexe, la probabilité d'erreurs humaines augmente – ce qui peut conduire involontairement à créer des brèches dans le système de sécurité.

Pour résumer, si les solutions isolées peuvent certainement être efficaces, elles sont aussi susceptibles d'entraîner un coût total de possession (TCO) extrêmement élevé.

BitDefender Business : amélioration de la sécurité et diminution du TCO

BitDefender Business a été conçu ex nihilo pour fournir une sécurité complète, de premier plan, au TCO le plus bas possible.

- **Faible TCO grâce à une productivité accrue.** Le prix d'achat d'un produit de sécurité ne représente qu'une faible part de son TCO comparé au coût de sa gestion et de sa maintenance. BitDefender Business a été structuré pour rendre l'administration aussi simple et fluide que possible et, par conséquent, son TCO est extrêmement bas.

  - ✓ **Politiques de sécurité.** BitDefender Management Server comprend une série de politiques de sécurité qui peuvent être facilement et rapidement implémentées en utilisant des modèles programmés personnalisables. Les politiques peuvent être utilisées pour contrôler chaque aspect du comportement de BitDefender, y compris le paramétrage de la planification des mises à jours et des processus anti-escroquerie, du pare-feu, de l'antispam, et pour spécifier la réponse à donner à chaque événement de sécurité ou de conformité. Les politiques hors connexion de BitDefender permettent aux administrateurs de vérifier que les ordinateurs sont toujours en conformité avec la politique, même quand ils sont déconnectés du réseau et ne communiquent pas avec le serveur d'administration. BitDefender peut également être configuré pour affecter une politique automatiquement sur n'importe quel ordinateur se connectant au réseau, par exemple en installant automatiquement le module client de BitDefender sur l'ordinateur, et en le bloquant jusqu'à ce qu'il ait atteint un état de conformité.

  - ✓ **Intégration à Active Directory (AD).** Les groupes créés dans AD peuvent être reproduits dans BitDefender Management Server et les politiques de sécurité affectées à chacun, permettant à l'entreprise de rentabiliser son investissement dans l'architecture réseau existante.

  - ✓ **Administration centralisée.** La console d'administration centralisée de BitDefender fait gagner du temps aux administrateurs en leur permettant de contrôler chaque module BitDefender à partir d'un unique emplacement.

L'administration rationalisée de BitDefender lui permet d'offrir un TCO extrêmement bas rapporté à une productivité accrue de l'administrateur.

- **Protection polyvalente intégrée.** BitDefender supprime le coût et la complexité associés à la maintenance de multiples produits isolés en intégrant tous les types de protection contre les virus, chevaux de Troie, rootkits, spyware, spam, arnaques de type phishing, attaques Zeroday et contre d'autres menaces dans une solution unique d'administration facile à utiliser.

Un avantage supplémentaire est que BitDefender permet aussi à l'entreprise d'éviter que son personnel abuse d'Internet. Des règles peuvent être paramétrées pour limiter ou interdire l'accès à des applications ou des sites Web connus pour comporter des risques liés à la sécurité ou à la productivité (par exemple des applications de messagerie instantanée ou des sites de réseaux sociaux). BitDefender offre une grande richesse de configuration ce qui permet à l'entreprise de choisir entre interdire complètement une application ou un site ou d'en limiter l'accès pendant certaines heures ou à certains groupes.

- **Flexibilité.** Contrairement à certaines solutions, qui deviennent peu pratiques quand le nombre d'ordinateurs administrés est important en raison des délais de communication client-serveur, la communication HTTP à sens unique qu'utilise BitDefender ne réclame que peu de ressources réseau. BitDefender peut donc s'adapter dans le temps aux nouveaux besoins de l'entreprise et permettre de renforcer l'expertise existante.

- **Sécurité de niveau international.** BitDefender propose une sécurité de premier plan. Les produits BitDefender ont reçu la certification ICSA et Checkmark, et de nombreuses récompenses VB100. En outre, BitDefender est connu pour avoir un des temps de réponse les plus rapides aux nouvelles menaces qui pèsent sur leurs clients.

Résumé

Confrontées à un terrain miné par des risques en constante évolution et augmentation, beaucoup d'organisations trouvent que leurs infrastructures de sécurité deviennent de plus en plus difficiles et coûteuses à gérer.

BitDefender apporte à ces organisations son concours pour simplifier leurs infrastructures de sécurité en renforçant leur protection contre les virus, les codes malveillants, le spam, le phishing et la protection du pare-feu en rassemblant toutes ces défenses en un Q.G. d'administration centralisée. En rationalisant l'administration de cette manière, BitDefender peut faire gagner à une organisation du temps et de l'argent. En outre, en permettant aux entreprises d'imposer une politique sur des appareils mobiles fréquemment déconnectés, BitDefender Business les aide à remporter le défi majeur d'aujourd'hui en termes de sécurité : la sécurisation des postes de travail.

Mais ce qui est encore plus important est qu'une organisation qui déploie BitDefender Business peut apprécier la tranquillité d'esprit que lui apporte la certitude de savoir que son réseau est entièrement protégé par l'une des solutions de sécurité de premier plan de BitDefender.

bitdefender

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

Références

1. Top Ten Cyber Security Menaces for 2008

http://www.sans.org/2008menaces/?utm_source=web-sans&utm_medium=text-ad&utm_content=text-link_2008menaces_homepage&utm_campaign=Top_10__Cyber_Security_Menaces_-_2008&ref=22218

2. Quantity of malware booms

http://www.heise-security.co.uk/news/101764/from/atom10

3. Gartner Survey Shows Phishing Attacks Escalated in 2007; More than $3 Billion Lost to These Attacks

http://www.gartner.com/it/page.jsp?id=565125

4. House Committee on Homeland Security Subcommittee on Emerging Threats, Cyber Security, and Science and Technology (statement of Donald R. Reid, Bureau of Diplomatic Security)

http://homeland.house.gov/SiteDocuments/20070419153111-10569.pdf

5. Industry Statistics (Ferris Research)

http://www.ferris.com/research-library/industry-statistics/

6. Microcap stock fraud

http://en.wikipedia.org/wiki/Microcap_stock_fraud

7. Security's Top Five Priorities

http://www.darkreading.com/document.asp?doc_id=123294

8. UK takes £6.5bn hit from Facebook & company

http://www.telegraph.co.uk/money/main.jhtml?xml=/money/2008/01/22/bcnface122.xml

9. Botnet

http://en.wikipedia.org/wiki/Botnet

10. Denial-of-service attack

http://en.wikipedia.org/wiki/Denial-of-service_attack

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