Emerging Threats to Business Security

WHITE PAPER

Now more than ever, businesses need to be concerned about the security of their networks. The number, variety and strength of the threats to computer and network security have dramatically increased and businesses need to be prepared against an ever-changing landscape of malware attacks.

Traditional security providers are focused on protecting computer applications. While this is certainly still important, today's biggest threats – as well as the most prominent emerging threats – are targeted at the emerging online lifestyle. With computer literacy increasing dramatically and the line between private and business use of computers and networks blurring, businesses need to keep a close eye on their employee's activities on their company networks and ensure that their network security is not at stake.

Threats to the Business Environment – Mobile Devices Latest Avenue for Attacks

In 2007, malware became one of the leading threats to network security. Malware is in constant flux and the only discernible trend right now is toward creating variants on existing pieces of malware, with ever-improving stealth capabilities and using them in more targeted attacks. There are numerous documented cases recently of targeted malware attacks against businesses (usually employing infected MSOffice files, though other techniques were also used). In each case, the malware used was written specifically for the occasion and saw little spreading beyond the initially-affected companies. As malware continues its surprise attacks, businesses should be on guard, especially as malware becomes increasingly sophisticated and continues to strike where businesses thought they were safe.

An area of significant concern for increasing malware attacks is in mobile devices. The use of smartphone technology has played a pivotal role in the threat's transition from multifunction, semi-stationary PCs to palm-sized "wearable" devices. The recent trend towards providing mobile devices with web browsers and always-on internet access has brought all the security concerns of the web to the mobile world and their connected enterprises. Viruses based on browser exploits will become common. As capabilities expand, security is traded for functionality, giving rise to a whole new class of opportunities for malicious attacks. Much like viruses on a computer, viruses on mobile devices can delete files, infect files, send private information from the mobile device, facilitate external attacks and/or drain the battery.

Businesses Best Defense Against Malware – Good Fences Make Good Neighbors

The old adage is – "good fences make good neighbors." That holds true today for businesses, though the fences in this case are security policies. Strong security policies coupled with the use of mobile antivirus (where applicable) should minimize the danger for business networks. Organizations need to recognize the immediate need to protect their employees' mobile devices from malware attacks that can significantly affect their network security. This security threat is significant and should lead businesses to consider deploying security solutions with a proven ability to detect new and previously unknown malware.

Other Threats in the Business Landscape – And How to Defend Against Them

Spyware remains a growing concern for businesses. In light of recently introduced data protection legislation in Europe and the United States, the danger to businesses in terms of liability for data theft/loss will remain high for the foreseeable future.

The various versions of "Storm Worm" still present the biggest single threat for the beginning of 2008, while the Zlob Trojan family is also being constantly improved and may become one of the major threats next year. Other such trojans, which create networks of infected computers and use them to spread viruses, spam or to perform denial of service attacks, may also surface. For businesses, firewalls remain a mainstay of network security when dealing with automated threats such as worms or botnets, when coupled with strong antivirus protection both at server and client levels.

Mass mailer viruses were still quite prevalent in the first half of 2007, but other threat categories are becoming more significant, although e-mail is still a preferred medium for other types of attacks.

Adware is seeing increasing use, as it carries lesser legal danger for the perpetrators. The productivity losses generated by cleanup are considerable, so businesses should consider implementing web filtering, to prevent infection with this and other types of malware.

With P2P file sharing already a commonplace thing, the number, diversity and impact of file infectors is bound to grow significantly in the next year. Disabling or limiting P2P traffic and other methods of file sharing, however, may carry productivity costs. Installing antivirus on every computer which shares files (be it a desktop or a fileserver) is highly recommended

Spam is diversifying and evolving, in hopes of avoiding spam filters by constant variation coupled with heavy obfuscation of both content and intent. Attachment spam, which has been on an overall decreasing trend in the last few months of 2007, is growing and may again become a significant concern in 2008. As productivity losses from spam are not negligible, SMBs should consider deploying antispam filters at both server and client levels.

Phishing (both web- and e-mail-based) is probably the worst current threat and will continue to remain so during the next year. It is also one of the most dangerous because it causes direct losses to victims (stolen bank accounts usually get "cleaned out" within hours or days). The most common type of phishing spam is based on threats to terminate the account being phished, while a second common variation is to ask a customer to enter their account info to "update the banking security app". The templates used to create these e-mails were generally very well-crafted and extremely similar to the web forms used by the target banks, although spelling mistakes and a web address different from that of the original bank were still apparent in many cases.

Phishing spam will continue to be significant (in volumes and damages alike) next year, with "improvements" expected in the techniques used to defeat antispam filters, as well as increasing use of SSL authentication by phishing websites (to get the all-important "lock icon" look in the victim's browser). The number of banks targeted is also expected to grow significantly. Anti-phishing is fast becoming a must-have feature for any sort of workstation security software.

Faced with an ever-increasing volume of new and existing threats, businesses should consider integrated security solutions which can be centrally deployed and managed and can be integrated in the existing security setup with a minimum of effort and expense. Organizations can no longer rely on basic network security to get the job done. The threats are more sophisticated and a company’s security needs to be as well.

Businesses need a security solution that assesses the type of activities in which users are engaged, as well as the channels employed to conduct those activities, to proactively determine where future threats are likely to arise and to ensure complete network security.

Bogdan Dumitru - Chief Technology Officer

About BitDefender

BitDefender is the creator of one of the industry's fastest and most effective lines of internationally certified security software. Since our inception in 2001, BitDefender has continued to raise the bar and set new standards in proactive threat prevention. Every day, BitDefender protects tens of millions of home and corporate users across the globe—giving them the peace of mind of knowing that their digital experiences will be secure. BitDefender solutions are distributed by a global network of value-added distribution and reseller partners in more than 100 countries worldwide.

More information is available at www.bitdefender.com.