



WatchGuard's Top Five Security Trends for 2009

27 January 2009 - With IT budgets under pressure, WatchGuard Technologies has identified the top five security trends to help businesses plan their security spending and stay one step ahead in 2009.

Trend 5 - Security and compliance collide

With 100 million stolen credit card accounts and massive chain-store failures to protect customer data, expect to see governments respond with substantive changes to security and identity protection laws, as well as tougher industry regulations, such as PCI DSS. Additionally, new lawsuits over internet privacy, malicious applications, unauthorized remote use of systems and IT resources, and data leakage will forge new legislation and set new precedents for years to follow.

Trend 4 - Botnets become stealthy

If 2008 was the year of botnets, expect to see 2009 to be the year botnets become stealthy. Learning from last year's lessons, botmasters will unleash new botnets of unparalleled sophistication and surprise. Based on quality, rather than quantity, botnets will become increasingly lucrative.

Trend 3 - Social networking gets ugly

Favourite social networking sites will transform into new platforms for launching web-based attacks, as well as for initiating new scams, phishing ploys and other tricks geared to get personal identification information.

Trend 2 - Increased attacks via SSL and HTTPS

As network systems become more adroit at blocking outside attacks and malware, criminals are becoming more skilled at delivering malicious payloads into networks. While SSL and HTTPS used to be safe and secure, they are now fertile fields for seeding these new attacks.

Trend 1 - The web puts everyone at risk

No longer will porn, gambling or other opprobrious sites host the usual hangouts for malware, spyware or other malicious applications. Instead, consumers will face new threats from trusted domains and everyday websites as they become silently infected with SQL injections or corrupted by drive-by downloads. Automated attacks will proliferate across the web targeting exposed, vulnerable machines and unwary users not expecting to see their favourite website as a potential threat.

“Criminals do not care if your IT budget is being cut this year,” said Eric Aarrestad, Vice President at WatchGuard Technologies. “They have one goal in mind, which is to get at your data, customer information, or to gain access to your computers, servers and network resources. By understanding where the next sets of threats will be, WatchGuard helps ensure businesses remain one step ahead of these risks.”

A podcast with more information is available at WatchGuard Radio Free Security:

<http://www.watchguard.com/education/radiofreesecurity.asp>

About WatchGuard Technologies, Inc.

Since 1996, WatchGuard has been building award-winning unified threat management (UTM) solutions that combine firewall, VPN and security services to protect networks and the businesses they power. Our newest appliances represent the next generation of network security: extensible threat management (XTM). All of our solutions feature reliable, all-in-one security, scaled and priced to meet the security needs of every sized enterprise. Our products are backed by 15,000 partners representing WatchGuard in 120 countries and more than a half million signature red WatchGuard security appliances have already been deployed worldwide in industries including healthcare, education, and retail. WatchGuard is headquartered in Seattle, Washington, with offices throughout North America, Europe, Asia Pacific, and Latin America.

To learn more, visit <http://www.watchguard.com/>.

Contacts:

Natasja de Groot
WatchGuard Technologies Inc
+ 31- 70 711 2085
natasja.degroot@watchguard.com

Allie Andrews
PRPR
+ 44 (0)1442 245030
allie@prpr.co.uk