WatchGuard Announces Top Five Security Trends To Impact 2009

Sydney – 28 January 2009 – WatchGuard Technologies, a global leader in extensible network security and connectivity solutions, has announced its top five critical security trends for 2009 with web security being the main battleground for concern in the year ahead.

At the same time, while malware and regulations continue to be top-of-mind issues for IT departments when it comes to network security, there is an absolute realisation among Australian businesses that, at some point, every organisation can be the target of an attack.

WatchGuard's top five security trends identify the following risks:

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 to host drive-by downloads. Automated attacks will proliferate across the Web that will impact exposed, vulnerable machines and unwary users not expecting to see their favourite website as a potential threat.

More Attacks via SSL / HTTPS

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

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.

Botnets with More Stealth

Although 2008 could be argued as the year of botnets, expect to see 2009 to be the year botnets become stealthy. Learning from last years lessons, botmasters will unleash new botnets of unparalleled sophistication and surprise. Their goal will be botnets of quality, not quantity as botnets become ever increasingly lucrative.

Security and Compliance Collide

Citing high profile examples of 100 million pilfered credit card accounts and massive chain-store failures to protect customer data, one thing is for certain, politicians will act. Expect to see substantive changes to security and identity protection laws, as well as toughened industry regulations, such as PCI DSS. Additionally, new lawsuits over internet privacy, malicious applications, unauthorised remote use of systems and IT resources, and data leakage will forge new legislation and set new precedents for years to follow.

"Criminals do not care if your IT budget is being cut this year," said Scott Robertson, ANZ Regional Director, 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."

About WatchGuard Technologies, Inc.

Since 1996, WatchGuard Technologies, Inc. has been the advanced technology leader of network security solutions, providing mission-critical security to hundreds of thousands of businesses worldwide. The WatchGuard Firebox X family of wired and wireless unified threat management appliances and WatchGuard SSL VPN remote access solutions provide extensible network security, unparalleled network visibility, management and control. WatchGuard products are backed by WatchGuard LiveSecurity Service, an innovative support, maintenance, and education program.

WatchGuard is headquartered in Seattle and has offices serving North America, Europe, Asia Pacific, and Latin America. To learn more, visit http://www.watchguard.com/ # # #