

New report highlights enterprise computing trends and network security impact analysis

Date: Mon, 10/18/2010 - 16:48

HP research enables companies to identify critical network vulnerabilities and protect enterprise assets



Stuart Hatto, EMEA Solutions, HP Networking, at Net Events EMEA Press Summit, Istanbul

HP recently published a research report that highlights enterprise computing trends and network security vulnerabilities for the first half of 2010, arming IT management with insight into potential data risks in the enterprise.

The report, by HP TippingPoint's Digital Vaccine Labs (DVLabs), gives enterprise organizations visibility into the attacks targeting their applications and underlying networks. This information allows administrators to make the system changes needed to reduce the possibility of network breaches that could lead to financial loss or decreased productivity. Employee use of web-based business applications and social networking sites while on corporate networks continues to grow daily. While the employee premise for these programs is honorable – to help build brand awareness or improve productivity – use of these applications opens up the enterprise network to serious security threats. The Cyber Security Risks Report uses real security event data to highlight how these activities put a network at risk so that businesses are better armed to address these concerns.

“To mitigate network security risk, organizations need insight into the potential threats associated with using social media networking sites and web application downloads in a business environment,” said Mike Dausin, manager, Advanced Security Intelligence, HP TippingPoint DVLabs. “By understanding the increased risk these applications pose to the

corporate network, organizations can implement remediation strategies to ensure that business processes, as well as data, remain secure.”

One of the key findings of the report was that more than 80 percent of network attacks targeted web-based systems. There are two key elements to this number: websites and web clients. The report shows websites are constantly at risk of being taken offline or defaced from SQL injection, PHP File Include or other attacks, and that these types of attacks have doubled in the last six months.

In addition, attacks against web browsers and web client applications such as QuickTime and Flash have tripled in the first half of the year and are often the main entry point for attackers to gain access to a network.

Understanding the attack frequency and the risks of web-based computing allows organizations to adjust security settings in their systems to protect the most critical assets on a network. In addition to these findings, the report will help organizations:

— Mitigate business risk by understanding Portable Document Format (PDF) flaws. Data from the report demonstrates how the structure of the application and its wide use in the enterprise makes it a very attractive target for attackers. This knowledge will help organizations tighten security controls around PDF use, helping prevent network compromise.

— Shut down attacks faster by identifying new techniques. The report highlights several covert and sophisticated techniques attackers use to hide their exploits. Armed with this knowledge, administrators can fine-tune their security practices for better protection.

— Prevent older threats from recurring by understanding their pervasiveness. Older security threats, such as SQL Slammer, Code Red and Conficker, still represent a significant source of attacks. Slammer, which originated in 2004, triggers HP TippingPoint IPS filters 10 times more than any other filter. Knowing this frequency and the likely causes, for example, pirated software, will allow administrators to make adjustments to network access or to monitor application purchasing, thereby helping to reduce risk to the entire system.

Methodology

HP TippingPoint DV Labs is a premier research organization for vulnerability analysis and discovery. It helps ensure clients have pre-emptive protection for vulnerabilities and zero-day attacks. The team applies cutting-edge engineering, reverse engineering and critical analysis to create comprehensive security filters that are automatically delivered to clients' intrusion prevention systems through the Digital Vaccine® service.

Event data from hundreds of deployed HP TippingPoint Intrusion Prevention Systems (IPS) was analyzed to identify the attacks. Event data refers to attack information that is collected when a security exploit triggers a particular filter in the HP TippingPoint IPS.

The following sources also contributed to the report:

— SANS, an organization dedicated to security training and certification;

— Open Source Vulnerability Database, an independent and open source database created by and for the community; and

— Qualys, which delivers on-demand IT security risk and compliance erability assessment and management products deployed in the field.

<http://www.telecomkh.com/en/business-communications/news/products-and-services/security/hewlett-packard/hp-tippingpoint-dvlabs/2393>