

Securing Network Endpoints Critical for Security

By Mitchell Ashley, CTO and VP Customer Experience

Originally published in The Boulder County Business Report, August 20, 2004

Your end users are under attack. Network security is being redefined just as businesses are bolstering their network security defenses with firewalls, intrusion detection/prevention (IDS/IPS) and good patching practices.

The Boulder County BUSINESS REPORT

Most businesses have suffered financial losses from worms, Trojans and spyware. A recent Aberdeen Group study reports that revenue losses attributed to Internet-based business disruptions now average \$2 million per incident, with almost one business disruption incident per organization per year. Mid-sized businesses (revenues of \$500M) experience a loss rate of over \$335,000 per incident. Even small businesses (\$10M in revenue) feel this impact with losses averaging \$6,700 per incident.

Once considered adequate for securing end-user PCs, antivirus software has proved it cannot prevent infection from worms, Trojans and spyware. Antivirus software should still be installed, but additional solutions are needed as well. A new kind of network security, called endpoint security, has emerged in the market to help protect businesses from the threat of end-user PC infection, both at work and at home.

Since mid-2003, a subtle but significant change has occurred in the way attackers attempt to breach our networks. The dirty little secret of network security is that the endpoint devices are not really secure, and attackers know it. The enormous number of worms, Trojans and spyware that have been introduced into the wild attests to this new approach. Network and security administrators are deluged by the many variants of Sasser, MyDoom, Netsky, Sober, Sobig, Bagle, Phatbot, Witty, Blaster and others.

There are two basic methods of breaking into any computer. The first is by exploiting operating system or application software that is improperly configured or that contains vulnerabilities that allow the device to be compromised. Many of the commonly deployed security defense systems are directed at preventing attacks of this nature by blocking malicious traffic or reporting known vulnerabilities that need to be repaired.

The second attack approach is to leverage end-user behavior. Many common and even desired end-user activities can be exploited to facilitate an attack. As a result, the attack bypasses traditional defenses such as firewalls and IDS/IPS solutions and has direct, immediate access to core network devices and other endpoints. By leveraging end users and their computers, hackers have an almost

unlimited number of unsecured corporate and home computers through which to gain access to our business and government networks.

How do the new worms and Trojans leverage the end user as part of the attack? In the case of MyDoom, malicious payload is delivered when end users open a Zip file. Sober.D relies on end users clicking a link to download a security patch contained in a would-be security e-mail bulletin, thereby delivering the worm directly to end users' devices. Unsuspecting end users then remotely connect to a network or connect their laptops to a network when returning to work and unknowingly infect it. This unfortunate disaster frequently requires security administrators to respond to the same attack multiple times.

Endpoint security solutions work to protect the network from unsecured and unknown devices. End users often knowingly or unknowingly disable security applications (such as antivirus or personal firewalls), neglect to install up-to-date security patches, improperly configure security settings or install restricted software (peer-to-peer, file-sharing or instant messaging). The reality of network security today is such that we cannot assume users can secure their own devices; endpoint devices must be considered suspect.

Endpoint security solutions protect against these dangers by prohibiting devices from accessing the network until they meet the necessary security requirements. They test laptops and PCs for compliance with the organization's security policy, checking antivirus software, personal firewalls, patches, security settings and required and restricted software. They also make sure the device has not already been compromised by worms, Trojans or spyware.

Devices that meet the security requirements are allowed access to the network. They are regularly retested while they are connected to ensure continued compliance. Those devices that fail compliance testing are quarantined, and their users are provided with direction and resources for updating the device with the necessary patches and security setting so compliance can be achieved. Ultimately, endpoint security solutions need to be deployed as organizations continue to leverage the efficiency and productivity inherent in the mobile workforce. Without it, companies will continue to be threatened by unpatched, outdated devices wreaking havoc on the network.

Mitchell Ashley is chief technology officer and vice president of Customer Experience at StillSecure, where he is responsible for the product strategy and development of the StillSecure suite of network security products. Ashley can be reached at mashley@stillsecure.com or (303) 381-3803.