

The Business Journal of Jacksonville - November 24, 2003

<http://jacksonville.bizjournals.com/jacksonville/stories/2003/11/24/smallb4.html>

# JACKSONVILLE Business Journal

## ENTERPRISE

### GUEST COLUMN

## Take steps to avoid 'blended threat' attacks

Andrew Reese

Blended threats represent the worst risk to computer security since the inception of computer viruses more than 20 years ago. Like the recent Blaster and Slammer worms, blended threats combine the most harmful characteristics of worms, viruses, Trojan horses and malicious code to exploit existing computer and Internet vulnerabilities.

These threats use multiple methods of propagation that can quickly defeat computer systems and networks that employ just one form of Internet security. When blended threats hit, they can spread rapidly and cause widespread damage.

Many blended threats require no human interaction to spread, which accounts for their almost unbelievable infection rate. In addition, blended threats are typically very malicious once they infiltrate and infect a computer. Slammer, for example, created a denial of service that caused servers to become inaccessible.

Blended threats are successful because many businesses implement only one form of computer security, such as a standalone antivirus product or a firewall. When blended threats encounter a single roadblock, they simply avoid it by using a different method to compromise the system.

Businesses must use a layered approach to computer security, referred to as security in-depth. From the client to the servers to the Internet gateway, security products should be implemented at all levels of the network. But too many companies have already learned the hard way that security technology alone cannot completely secure a network. In addition, workers should be trained regularly on how to identify and avoid today's sophisticated Internet threats.

The following security policies are examples of how companies can increase the security of their networks by reducing the likelihood of a network breach:

- Protect passwords -- Some computers and networks are protected by passwords as a security precaution. Passwords, however, can be a major vulnerability. It's not unusual for people to try to save time by sharing passwords or choosing a simple password, which make it easy for unauthorized users to gain access.

Passwords should be randomly chosen and should not be names or important dates. A good password will be at least six characters long, including both letters and numbers. A policy that requires users to change their passwords regularly also reduces the risk of a system breach.

- Remove unnecessary services -- Eliminating unneeded services can dramatically reduce system vulnerability. Organizations need to determine which services they truly require and remove any that are unnecessary.
- Use integrated security hardware and Software -- Avoid using security products from different

manufacturers since they may not be designed to properly overlap, leaving holes that blended threats may exploit. Security technology works best when layered across all parts of the network.

Most major security vendors such as Symantec Corp. offer complete security solutions that are designed and tested to work together without leaving any gaps in security coverage.

- Keep patches current -- The majority of blended threats are based on known vulnerabilities. Keeping operating systems, applications and security products up-to-date with the latest security patches will reduce the chances of a blended threat entering from Web pages or e-mail. These patches are available from the vendor and they will seal off many holes blended threats use to spread.

Blended threats are expected to appear with increased regularity and growing complexity. The best defense against today's threats consists of adopting best practices and applying them in concert with comprehensive security solutions.

Although the specific policies and products required to combat blended threats will vary depending on the size and needs of each individual company, every organization should make provisions to implement an integrated security approach that combines layered security products with educated, aware employees. Failure to address blended threats properly may leave your systems and networks vulnerable to exploitation.

*Andrew Reese is national director of Security Consulting at DynTek Inc. [jacksonville@bizjournals.com](mailto:jacksonville@bizjournals.com) / 396-3502*

© 2003 American City Business Journals Inc.

→ [Web reprint information](#)

*All contents of this site © American City Business Journals Inc. All rights reserved.*