



THE ILLUSION OF INFORMATION SECURITY

by Blaine Berger, President of Electronic Oasis Consulting, Inc.

Most organizations today have implemented firewalls to protect their networks from Internet-connected threats. The protection offered by a firewall, however, can be a dangerous illusion. Consider that many popular and freely available applications such as instant messaging, peer-to-peer file sharing, game play and remote control software are quite popular with users inside many organizations. What's not recognized is that many of these applications adapt themselves to firewalls and are not easily controlled with technology alone. All of these applications can be user-installed without the knowledge or permission of your Information Technology staff.

For example, did you know that one popular Internet poker game can collect the information on your computer screen? It's not illegal because users authorize this by agreeing to the terms and conditions when downloading and installing the game.

WHAT ARE THE RISKS TO YOUR ORGANIZATION ?

Many of these tools provide the users with benefits, but what is the threat to your organization from these popular applications?

- The unintended sharing of your organization's information
- An entry point for viruses and Trojan horse infections
- Consumption of bandwidth – especially if music files and pictures are being exchanged
- Unexplained poor PC performance
- Employee productivity losses from excessive Instant Messaging chatting and interruptions

There have been cases where unsuspecting users had thousands of Internet users retrieving popular songs from their computers and slowing the performance of their machines and their organization's Internet connection considerably. Remote control software (such as GoToMyPC, PC Anywhere, and VNC) is problematic because it represents a point of weakness that can be exploited to gain undetected access to your network and resources.

IS THE FIREWALL ENOUGH?

A firewall is like the fence around your house. Its purpose is to protect a perimeter while still allowing access for permitted traffic. If you don't have a firewall, it's a good bet that you have one or more compromised computers. Even with a firewall, however, your computer systems and the information they contain are not as safe as you might think.

How do you know if your firewall is properly configured to do its job? Have you kept up with the security updates to the firewall? Do you have additional protection beyond your firewall – an alarm system that can alert you to threats that bypass the firewall or originate inside your company?

Copyright 2005 Electronic Oasis Consulting, Inc. All Rights Reserved

This copy is for your personal, non-commercial use only. Distribution and use of this material are governed by copyright law. For publication information, please contact Electronic Oasis Consulting, Inc. at 1-303-415-0777 or e-mail publication@e-oasis.com.

GATHER THE LOW-HANGING FRUIT

What can you do to address the continuous emergence of adaptive threats without spending a fortune doing it? Use common sense and a systematic approach to your organization's security. All of the following steps represent low-hanging fruit with steps you can implement in your organization before spending money on a study that recommends the obvious.

- Document and Enforce Acceptable Use Policies
Policies which explain what applications are acceptable form the basis for action when violations are detected.
- Invest in a Spam Blocking Solution
Increasingly, e-mail is used as the transport to deliver threats directly to your users. Blocking spam and attachments will help you eliminate this risk.
- Educate your users via email about the risks
Regular emails can be very effective in helping users understand risks of high-risk applications and recognize the symptoms of a compromised PC.
- Segment your network into different security zones
Consider segregating your user's computers from the servers they access on a different network segment. You can more easily apply a tighter security policy and monitoring to prevent the unauthorized access of your customer's accounts by preventing exploitation and compromises of your servers.
- Mandate the use of virus scanning on every machine
This simple change will save hours of labor by preventing infections, data loss, and labor-intensive diagnostic and restore efforts.
- Inspect and verify your firewall configuration regularly
Having a third party inspect your firewall configuration is like inspecting your fence for holes. It's simple, cost-effective and pays big benefits when holes are patched before they are exploited.
- Educate yourself about Intrusion Detection Systems (IDS)
An IDS can listen on your network and alert you when it detects a threat.
- Conduct an automated software audit of every machine on a regular basis
An up-to-date searchable inventory of installed software makes identification of rouge programs and harmful applications easier.

NOTHING CONCENTRATES THE MIND LIKE A HANGING

An interesting anecdote asserts that many organizations spend more money on coffee services than they spend on information security. Another old adage states that "*Nothing concentrates the mind like a hanging*". Applied to security, it typically takes a breach or crisis before an organization reacts to a threat.

The media is filled with accounts of missing data, misplaced computers, serious security breaches, and the collateral damage to an organization's reputation that may take years to repair. Can your company afford these costs? The two biggest mistakes to avoid are:

1. Failing to adequately budget for information security to protect your company
2. Failing to use outside help to validate the security measures you do have

Finally, it's important to stay vigilant and apply policy and technology changes quickly to address threats. Information security can be a dangerous illusion when you remain unaware of the threats and counter-measures.

To comment on this article or suggest future topics, contact Blaine Berger via e-mail blaine@e-oasis.com or phone 303-415-077. Electronic Oasis Consulting, Inc., "The Network Specialists", provides expert network and security services. See <http://www.e-oasis.com> for more information.

Copyright 2005 Electronic Oasis Consulting, Inc. All Rights Reserved

This copy is for your personal, non-commercial use only. Distribution and use of this material are governed by copyright law. For publication information, please contact Electronic Oasis Consulting, Inc. at 1-303-415-0777 or e-mail publication@e-oasis.com.