



Browsing With A Loaded Gun:

A strong Web Security Policy is key to keeping your company safe in the Net-centric world

Copyright 2000 PentaSafe Security Technologies, Inc. All rights reserved.

About PentaSafe Security Technologies, Inc.:

PentaSafe provides software solutions that secure and protect the operating systems, applications, and data that drive the digital economy. PentaSafe VigilEnt Security Management Solutions allow companies, for the first time, to audit, assess vulnerabilities, define security policies, implement and manage security across a mixed corporate IT environment from a single point of control. By bringing the components of the new digital infrastructure under common control, PentaSafe allows companies to quickly and efficiently secure and maintain the state of constant security compliance required to successfully interact with customers and partners.

Corporate Web site: www.pentasafe.com

The information in this document is subject to change without notice and must not be construed as a commitment on the part of PentaSafe Security Technologies, Inc. PentaSafe assumes no responsibility for any errors that may appear in this document. The software described in this document is furnished under a license and may be used or copied only in accordance with the terms of the license. No part of this document may be reproduced, stored in retrieval system, or transmitted in any form or by any means without the prior written permission of the copyright owner.

PentaSafe is a registered trademark of PentaSafe Security Technologies, Inc. All other product names or brand names may be trademarks or registered trademarks of their respective holders. Product names or brand names may trademarks or registered trademarks of their respective holders.

Browsing with a Loaded Gun:

A strong Web Security Policy is key to keeping your company safe in the Net-centric world.

In ancient Internet times, the browser was a handy tool for exploring the wild world of the Web. Then came the corporate Intranet, and suddenly we could search the phonebook and maybe even change our benefits online. Soon Web applications muscled in on client-server. And now we have Application Service Providers (ASP) promising to provide Web-based access into virtually any business system: ERP, payroll, HR and accounting. In the last three years, the once-lowly Web browser has changed from a cute toy to an indispensable tool for doing business.

But while the browser has gained in importance, it has been virtually ignored as a security threat. Although some companies have policies restricting where users can browse, few have policies that address browser security. And the risk may be greater than you think.

How can my Web browser be a security risk? There are dozens of ways Web browsers can be compromised to give critical information out or allow malicious files in. Generally, browser security holes fall into two broad categories: browser bugs and user error. Bugs are fixed with patches; user errors require policy and education.

Browser Bugs

As browsers become more "functional," each release gets more complex and may open new security holes. Over the years, both Netscape and Internet Explorer have been vulnerable. Breaches can be small, such as a system crash, or huge, like introducing a virus or accidentally giving a username and password to a hacker.

For example, bugs in Netscape Navigator 4.0 could allow a malicious Web site to hijack any files from your computer. Another bug in Netscape Navigator 4.0 through 4.04 contains a security hole involving JavaScript programs that could access browser preferences settings. In many cases, these settings include e-mail addresses, accounts and passwords. Since many user accounts are the same as their e-mail addresses, this opens a potentially large hole in your network.

Another hack effecting Internet Explorer uses JavaScript to create an invisible frame 1x1 pixel wide. While the unsuspecting user browses a remote site, a JavaScript program running in the invisible frame scans the user's local machine and file shares for files with well-known names; it may then upload them to any site on the Internet. Both Microsoft and Netscape promptly fixed these bugs. But unless you apply the patches before the hackers exploit them, you are vulnerable.

User Errors

While software bugs can open security holes, larger threats arise from ignorance. There is only so much that technology can do. Many security lapses occur because users are unaware of security issues.

For example, with a single click users may download and run any executable program from any Web site. While some security policies prohibit downloads, they happen more than you might think. Cute executables such as dancing "e-cards" can be disguises for Trojan Executables, programs that run maliciously in the background destroying data while the user watches in ignorance.

Another risky end-user mistake is improper browser security settings. For example, browser versions of Internet Explorer 4.0 and above allow you to specify security in several different "zones." The problem is that there are over 20 options for each zone! Most users have no idea what these settings mean or of the consequences of changing them.

Another less obvious but very serious security issue involves new features built in Internet Explorer 5.0. IE has a function that will save the values of form fields on any Web site you visit. When you return to that site it can auto-complete the form, including your password! Thus if you accessed the corporate Payroll system and left your PC on while you were at lunch, anybody who uses your browser has one-click access into payroll.

Finally, one of the most damaging ways to misuse your browser is with "external viewers." These are programs that are launched by the Web browser to view files in other formats besides HTML. If your Intranet uses Internet Explorer, the default viewer for Word and Excel files is Microsoft Office. This feature is great for distributing documents on a corporate Intranet. But it also means that any .doc file downloaded from the Internet will launch MS Word—a great way to distribute harmful Word or Excel macro viruses into your network.

What can you do?

The Policy Defense: Any good security defense begins with your security policy. Make sure that your Policy covers appropriate use of the Web browser as a business tool. Here are some key items that your policy should address:

- ❑ **Keep browser versions up to date**

Make it a policy that all users have the most recent versions and security patches of your standard browser. If you don't have a browser standard, pick one and add that to your policy. It's easier to chase one set of patches than two. Both Netscape and Microsoft post security alerts and patches on their Web sites.

- ❑ **Enable screen savers with passwords**

This is the simplest way to secure your desktop and reduce the chances of someone else accessing corporate data from your PC.

- ❑ **Pick standard security settings**

Set standards for your Web browser Security settings and make it a policy to periodically audit or enforce these settings. System management tools like SMS or WinInstall can help enforce settings across the desktops. If you can't do it automatically, then have your IS department do periodic spot checks.

- ❑ **Do not use your passwords on the public Internet**

How many of your users have the same password on their E*trade account, Yahoo, mail and your corporate LAN?

- ❑ **Buy an active screening tool**

There is hope even for the most paranoid among you. Vendors now provide software that intercepts any content that comes through the firewall and attempts to analyze it for harmful programs. Other software can intercept and scan e-mail for viruses or specific content before it reaches your end-users. These pro-active approaches require investment, but increase the overall security of your network.

User education

Make it a policy to educate your users on the dangers of browsing in ignorance. Most corporations provide little or no security training. Make sure employees understand the policy on Web browsing. Provide clear examples of improper actions. Help them understand the risks of "external" viewers, and of downloading executables from the Web. A policy is only as effective as the people who follow it. Chances are, some of your users are browsing with a loaded gun. Don't let them shoot you in the foot.

Sidebar Quote:

"In the first six months of 1999, U.S. businesses experienced \$7.6 billion in losses as a result of disabled computers due to malicious code traveling through the public Internet, according to consulting firm Computer Economics, Inc."

Contact Information

PentaSafe Corporate Headquarters:

PentaSafe Security Technologies, Inc.
802 Lovett Boulevard
Houston, Texas 77006 USA

Toll Free: 1- 888-400-2834
Int'l: +1-713-523-1992
Email: info@pentasafe.com

International Offices:

PentaSafe France
17 Square Edouard VII
75009 Paris France

Phone: +33 (0) 1 53 43 90 53
Fax: +33 (0) 1 53 43 90 54
Email: info.france@pentasafe.com

PentaSafe Denmark
Kirke Vaerloseevej 18A
DK-3500 Vaerlose
Denmark

Phone: +45 4420 9858
Fax: +45 4420 9868
Email: info@pentasafe.co.uk

PentaSafe United Kingdom
Postford Mill
Chilworth, Surrey
GU4 8RT

Phone: +44 (0) 8700 765400
Fax: +44 (0) 8700 765401
Email: info@pentasafe.co.uk

PentaSafe Germany
Frankfurter Strasse 23363263
Neu-Isenburg
Germany

