



Procinct Security

SYSTEM HARDENING

"In 2002, the total financial losses [due to viruses, worms, etc.] reported increased from \$45,288,600 to \$49,979,000 with an increase in the average loss from \$243,845 per organization in 2001 to \$283,000 per organization in 2002."

Source: Computer Security Institute/FBI, "2002 Computer Crime and Security Survey"

What is System Hardening?

Every company has at least one server that is considered a critical resource, whether it's an e-Commerce web server, an internal database server with customer credit card information, or a mail server that houses confidential corporate communication. Unfortunately, most out-of-the-box applications and operating systems do not adequately protect your information assets. Because of this, companies need to harden their systems to ensure that the applications, software, and information on them are protected.

Hardening systems is a defensive strategy that protects against attacks by removing vulnerable and unnecessary services, patching security holes, and securing access controls. This process includes evaluating a company's security architecture and auditing the configuration of their systems in order to develop and deploy hardening procedures to secure their critical resources. These procedures are customized for each business, updated as threats evolve, and automated for easy deployment and auditing.

Both hackers and their tools are becoming more and more sophisticated and ubiquitous, forcing companies to ensure that their systems are constantly up-to-date to defend against new attacks. By hardening systems, your company can further protect itself against the financial losses associated with system downtime, lost ad revenue, theft of intellectual property, theft of customer information, and negative publicity.

How can System Hardening help your company?

Our comprehensive System Hardening service helps your company accomplish the following:

- Ensure that critical resources have up-to-date patches and are able to defend against known vulnerabilities
- Enable rapid deployment of a secure baseline configuration and easy auditing of a server for unexpected changes.
- Improve your systems' security as much as possible in anticipation of an upcoming internal 3rd Party audit before any type of security testing is performed.
- Ensure business continuity by preventing viruses and Trojans from spreading on your systems.
- Reduce the risks associated with malice and human error.

Procinct Security Professional Services

Procinct Security provides a wide range of security consulting services:

- | | |
|---------------------------------------|---------------------|
| Network Vulnerability Testing | Incident Response |
| Web Application Security Review | Penetration Testing |
| Independent Verification & Validation | Risk Assessment |
| Policies & Procedures Development | System Hardening |

Proven success with Procinct Security

We automate paying attentionSM. Procinct Security Corporation is dedicated to developing cutting edge information security solutions that help clients across all industries secure their Internet infrastructure. Procinct Security, provider of the ProSentryTM Internet Security Monitoring service, is comprised of senior software architects and trustworthy security professionals who hold sensitive security clearances and CISSP and SANS GIAC security certifications. Procinct Security also provides a wide range of security consulting services.

Procinct Security is a charter member of the Center for Internet Security and an independent member of the BDO Seidman Alliance. For more information email info@procinct.com or sales@procinct.com.

AN INDEPENDENT MEMBER OF



THE CENTER FOR
INTERNET SECURITYSM
CHARTER MEMBER



Procinct
SECURITY

870 Market Street, Suite 1105
San Francisco, CA 94102
Phone 415.395.2945
Fax 415.296.8642
sales@procinct.com
www.procinct.com