

Issue 5

Publication Date: 13/01/06

Contents

- CERT® Security Improvement Modules
- Security Flaws on the Rise, Questions Remain
- Protecting Your Core: Infrastructure Protection Access Control Lists
- Insider Threat Study
- NISCC Quarterly Review (Q04/2005)
- Windows Rootkits of 2005, Part Three
- Preventing and Responding to Identity Theft
- Regaining Control

CCIP Contact Details:

T: +64 (0)4 498-7654
F: +64 (0)4 498-7655
E: info@ccip.govt.nz

<http://www.ccip.govt.nz>

CERT® Security Improvement Modules

CERT/CC

Each CERT Security Improvement module addresses an important but narrowly defined problem in network security. It provides guidance to help organizations improve the security of their networked computer systems.

Each module page links to a series of practices and implementations. Practices describe the choices and issues that must be addressed to solve a network security problem. Implementations describe tasks that implement recommendations described in the practices. Please note that these implementations should be considered examples; they have not been updated to reflect current versions of operating systems or current vulnerabilities.

Source: <http://www.cert.org/security-improvement/index.html>

Security Flaws on the Rise, Questions Remain

Security Focus

After three years of modest or no gains, the number of publicly reported vulnerabilities jumped in 2005, boosted by easy-to-find bugs in Web applications. Yet, questions remain about the value of analyzing current databases, whose data rarely correlates easily.

Source: <http://www.securityfocus.com/print/news/11367>

Protecting Your Core: Infrastructure Protection Access Control Lists

Cisco Systems

This document presents guidelines and recommended deployment techniques for infrastructure protection access control lists (ACLs). Infrastructure ACLs are used to minimize the risk and effectiveness of direct infrastructure attack by explicitly permitting only authorized traffic to the infrastructure equipment while permitting all other transit traffic.

Source: <http://www.cisco.com/warp/public/707/iacl.html>

Insider Threat Study

US Secret Service & CERT/CC

In August 2004, the U.S. Secret Service and Carnegie Mellon University Software Engineering Institute's CERT® Coordination Center (CERT/CC) announced the findings of the first Insider Threat Study report, a collaborative effort to better understand insider activities affecting information systems and data in critical infrastructure sectors.

The first report focuses on the people who have had access to and have perpetrated harm using information systems in the banking and finance sector, which includes credit unions and financial institutions. This study, made possible by significant financial support from the Department of Homeland Security's Science and Technology Directorate, is the first of its kind to provide a comprehensive analysis of insider actions by analyzing both the behavioral and technical aspects of the threats.

The findings underscore the importance of organizations' technology, policies and procedures in securing their networks against insider threats, as most of the cases

Continued overleaf...

Information Security Links

- National Infrastructure Security Co-ordination Centre (NISCC)
- Public Safety and Emergency Preparedness Canada (PSEPC)
- United States Computer Emergency Readiness Team (US-CERT)
- CERT Coordination Center (CERT/CC)
- Australian Computer Emergency Response Team (AusCERT)
- Internet Storm Center (ISC)
- US-CERT Cyber Security Bulletins

Safe Computing Links

- The Internet Safety Group (NZ)
- CCIP Security Tips
- National Cyber Alert System (USA)
- AusCERT National Information Technology Alert Service (AUS)
- IT Security Awareness For Everyone (UK)
- National Alerting Service (Netherlands)

Subscribe

Subscribe to this e-bulletin and other CCIP publications, alerts and advisories by emailing "subscribe" to publications@ccip.govt.nz



Insider Threat continued.

showcased in the report were perpetrated by insiders with minimal technical skills. Various proactive practices are among the suggestions offered by the report.

Source: http://www.secretservice.gov/ntac_its.shtml

NISCC Quarterly Review (Q04/2005)

UK National Infrastructure Security Co-ordination Centre

In this issue we look at the factors that determine national criticality. There is also a report from the recent SANS Top 20 launch held in London and NISCC assesses the threat of electronic attack in the coming year. We also cover the First Responders' workshops, outline some of the agreements from the recent Meridian conference and provide an introduction to an academic research paper on the drivers for information sharing.

Source: <http://www.uniras.gov.uk/niscc/docs/re-20051230-01143.pdf?lang=en>

Windows Rootkits of 2005, Part Three

Security Focus

The third and final article in this series explores five different rootkit detection techniques used to discover Windows rootkit deployments. Additionally, nine different tools designed for administrators are discussed.

Source: <http://www.securityfocus.com/print/infocus/1854>

Preventing and Responding to Identity Theft

US-CERT

You can be a victim of identity theft even if you never use a computer. Malicious people may be able to obtain personal information (such as credit card numbers, phone numbers, account numbers, and addresses) by stealing your wallet, overhearing a phone conversation, rummaging through your trash (a practice known as dumpster diving), or picking up a receipt at a restaurant that has your account number on it. If a thief has enough information, he or she may be able to impersonate you to purchase items, open new accounts, or apply for loans.

The internet has made it easier for thieves to obtain personal and financial data. Most companies and other institutions store information about their clients in databases; if a thief can access that database, he or she can obtain information about many people at once rather than focus on one person at a time. The internet has also made it easier for thieves to sell or trade the information, making it more difficult for law enforcement to identify and apprehend the criminals.

Source: <http://www.us-cert.gov/cas/tips/ST05-019pr.html>

Regaining Control

Security Focus

Securing endpoint systems by locking them down using complex software brings back memories of another era, where business computers were once used for business applications only - and businesses retained control over their assets and data.

Source: <http://www.securityfocus.com/print/columnists/372>

While this e-bulletin is accurate to the best of our knowledge, CCIP does not accept any responsibility for errors or omissions. If any of the vulnerabilities affects you, you are advised to ensure that you have the most current information available. CCIP will not be liable for any loss or damage howsoever caused, arising from or in connection with the use of information contained in this e-bulletin.

CCIP only issues those external alerts that we assess as serious and would affect a large number of New Zealand users. For notification of all discovered software vulnerabilities we recommend that you subscribe to a commercial Computer Emergency Response Team or to vendor alert lists.

Reference in this e-bulletin in any manner to any commercial product, process or service does not constitute or imply its endorsement or recommendation by CCIP. Views and opinions expressed herein may not be used for advertising or product endorsement purposes.