



AGAINST CYBER THREATS

CCIP e-Bulletin

CENTRE *for* CRITICAL INFRASTRUCTURE PROTECTION

Issue 36

Publication date: 30/03/07

Contents

- Windows Server 2003 Service Pack 2
- NIST Releases Guidance Document for Risk Mitigation Planning
- 50 Things I Wish I'd Known Before... Becoming a CIO
- The Dirty Dozen: Killing False Positives
- Mapping the Mal Web
- Internet Security Threat Report
- Malware Disrupts Half Of Global Business, Study Finds
- Security & Risk: The Defense Never Rests

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/>

Windows Server 2003 Service Pack 2

Microsoft

Microsoft Windows Server 2003 Service Pack 2 (SP2) is a cumulative service pack that includes the latest updates and provides enhancements to security and stability, including:

- The ability to simplify the creation and maintenance of the Internet Protocol security (IPsec) policy
- Group Policy support for non-broadcasting networks and Wi-Fi Protected Access 2 (WPA2) settings to allow Windows wireless client configuration
- Windows wireless client support for WPA2 with the following features:
- Non-broadcast network profiles are now marked with a flag to improve the security of the Windows wireless client
- Windows will not automatically connect to a peer-to-peer network, even if it has been automatically saved in the preferred network list

Source: <http://www.microsoft.com/>

NIST Releases Guidance Document for Risk Mitigation Planning

US National Institute of Science and Technology

NISTIR 7390 provides an annotated bibliography of printed and electronic resources that serves as a central source of data and tools to help the owners, managers, and designers of constructed facilities develop a cost-effective risk mitigation plan. NISTIR 7390 supports the use of the Cost-Effectiveness Tool for Capital Asset Protection by providing information on key resources needed to perform a rigorous economic evaluation.

Source: <http://www2.bfrl.nist.gov/>

50 Things I Wish I'd Known Before... Becoming a CIO

CIO Magazine

Don't miss this exclusive insight by Paul Coby, BA's CIO and one of the UK's leading industry figures.

"The journey has been challenging, exciting and nerve-wracking. I've learnt a lot on the way and the '50 things' is the result of painful, sometimes harmful and occasionally (almost) disastrous mistakes. Some are funny in retrospect; some still freeze my blood."

Source: <http://www.cio.co.uk/>

The Dirty Dozen: Killing False Positives

IT_Observer

In the classic war movie *The Dirty Dozen*, Lee Marvin's maverick major must make a crack fighting unit from an unruly squad of prisoners, then launch an all-out assault behind enemy lines. It's a near-impossible assignment.

Any IT director trying to battle security threats to their networks day after day will know the feeling. Maintaining a clear view of their true security position is a constant, enervating battle, devouring man-hours and resources.

Source: <http://www.it-observer.com/>

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)

Mapping the Mal Web

McAfee

Online safety risks are a truly global issue. Yet differences in threats vary significantly by country and other factors, for example:

- A consumer is almost 12 times more likely to encounter a drive-by-download while surfing Russian domains as Columbian ones.
- Registering at a Web site in India results in a 4.3% chance of getting spammy e-mail. Taking the same action with a domain registered in China yields a 7.2% chance.
- 5.2% of Vietnamese Web sites have risky downloads. Just 0.5% of Singaporean sites host such files.
- 2.7 million times every month, casual Web surfers visit risky Dutch Web sites. Even though Hong Kong has approximately the same percentage of risky Web sites, those risky domains receive just 52,000 clicks each month.

Source: <http://www.siteadvisor.com/>

Internet Security Threat Report

Symantec

The latest Internet Security Threat Report released today by Symantec Corp. (Nasdaq: SYMC) reveals that the current Internet threat environment is characterized by an increase in data theft, data leakage, and the creation of targeted, malicious code for the purpose of stealing confidential information that can be used for financial gain. Cyber criminals continue to refine their attack methods in an attempt to remain undetected and to create global, cooperative networks to support the ongoing growth of criminal activity.

Source: <http://www.symantec.com/>

Malware Disrupts Half Of Global Business, Study Finds

InformationWeek

Malware is disrupting nearly half of worldwide businesses, a new study reports. The Webroot State of Internet Security study reports that out of 600 global businesses that were surveyed, 43% of them said they're suffering business disruptions due to malware and more than 60% do not have an information security plan.

Source: <http://www.informationweek.com/>

Security & Risk: The Defense Never Rests

CIO Insight

There is no choice: Eternal vigilance against clever hackers, greedy cybercriminals and clueless employees is part of the cost of doing business. But companies can still choose how they defend themselves. Some companies are moving away from Microsoft products. Others have started to treat security as a risk management issue rather than an IT problem: Instead of being a function that installs firewalls and enforces rules, IT security has become part of an overarching strategy of minimizing strategic and legal risks. So far, this broader approach to security is working. Meanwhile, compliance is coming to the end of its run as an urgent priority, since most companies have achieved compliance with the Sarbanes-Oxley Act. But there is an important carry-over effect: Companies are still upgrading their financial systems and processes. Most IT executives believe there are still plenty of opportunities for automating the finance function.

Source: <http://www.cioinsight.com/>



AGAINST CYBER THREATS

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.