



AGAINST CYBER THREATS

CCIP e-Bulletin

CENTRE for CRITICAL INFRASTRUCTURE PROTECTION

Issue 34

Publication date: 02/03/07

Contents

- Application for a New 2LD - bank.nz
- Three Important New NIST.GOV SP800 Documents Released
- Writing an RFP for a Network Access Control Solution
- Penetration Testing and Vulnerability Analysis are both Essential to Ensure Web Application Security
- NIST Releases Info Security Documents
- Watchfire Discovers Google Desktop Vulnerability
- Google Desktop Hole Closed - For Now
- Self-Healing Networks, Myth or Reality?
- How Does the Hacker Economy Work?

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/>

Application for a New 2LD - bank.nz

Office of the Domain Name Commissioner

An application has been received to create a new, moderated second level domain (2LD) – bank.nz. Comments are sought on the application, and on the moderation policy that will be used to accept registrations. In particular, comment is sought on how the application met the criteria for a new 2LD.

Source: <http://www.dnc.org.nz/>

Three Important New NIST.GOV SP800 Documents Released

US National Institute of Science and Technology

NIST.GOV has released three new SP800 documents covering securing email, IDS/IPS Systems, and securing wireless with 802.11i

Source: <http://www.nist.org/>

Writing an RFP for a Network Access Control Solution

IT-Observor

When considering network security solutions, many organizations choose network access control (NAC) technology as an integral part of their security fabric. Many industry experts believe that NAC is vital to complete network security. NAC helps to ensure that devices entering the network will not introduce viruses or other potentially debilitating malware. Once devices have been risk-assessed and admitted to the network, NAC continuously monitors their activity the entire time they are on the network.

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

Penetration Testing and Vulnerability Analysis are both Essential to Ensure Web Application Security

SecurityPark.net

People often ask the question “should I use vulnerability analysis tools to assess my web based applications or should I look to penetration testing?” As an industry, we may be asking the wrong question. First, let’s look at how the web application industry has grown over the years and how penetration testing has scaled to meet that challenge.

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

NIST Releases Info Security Documents

Government Computer News

The National Institute of Standards and Technology has published two new interagency reports designed to help auditors, inspectors general and senior management understand and evaluate information security programs.

NISTIR 7359, titled “Information Security Guide for Government Executives,” is an overview of IT security concepts that senior management should grasp. NISTIR 7358, titled “Program Review for Information Security Management Assistance (PRISMA),” lays out a standardized approach for measuring the maturity of an information security program.

Source: <http://www.gcn.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)

Watchfire Discovers Google Desktop Vulnerability

Watchfire

Web application security leader Watchfire, today announced its security researchers have discovered a vulnerability in Google Desktop which could enable a malicious individual to achieve not only remote, persistent access to sensitive data, but in some conditions full system control.

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

Google Desktop Hole Closed - For Now

Techworld

Google has closed a cross-site scripting vulnerability, through which Google Desktop could give attackers remote control of a victim's computer and its contents - but security experts warn there is more to come.

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

Self-Healing Networks, Myth or Reality?

SecurityPark.net

Until now, network security has acted mainly as a device to police the system, with only the power to announce that the intruder is in the building, but has lacked the ability to respond dynamically to turf them out and repair any damage they may have done without manual intervention.

But how close are we to achieving self-healing network? Like any good vaccine, a proven solution must be able to eliminate the spread of disastrous security events impacting the business such as worms, viruses or DDoS attacks.

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

How Does the Hacker Economy Work?

InformationWeek

When retailer TJX disclosed Jan. 17 that the computer systems that store data related to credit card, debit card, check, and merchandise return transactions had been broken into, it said it had discovered the hack in December. But security officials at Visa had been seeing an increase in fraudulent activity on credit and debit cards related to TJX properties, such as T.J. Maxx, Marshalls, and HomeGoods stores, since mid-November. That means it's possible the purloined consumer data has been floating around the Internet, available for purchase on black market Web sites and chat rooms, for at least two months, maybe longer.

Hacking isn't a kid's game anymore. It's big business. Online black markets are flush with stolen credit card data, driver's license numbers, and malware, the programs that let hackers exploit the security weaknesses of commercial software. Cybercriminals have become an organized bunch; they use peer-to-peer payment systems just like they're buying and selling on eBay, and they're not afraid to work together.

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