



AGAINST CYBER THREATS

CCIP e-Bulletin

CENTRE *for* CRITICAL INFRASTRUCTURE PROTECTION

Issue 33

Publication date: 16/02/07

Contents

- The Psychology of Security
- Fundamental Computer Investigation Guide for Windows
- PHP Security from the Inside
- Guide to Computer Security Log Management
- Trends in Malware Threats
- Organized malware factories threaten Internet users
- IPv4 Countdown Policy Proposal
- Hardening Microsoft Windows – STIGS, Baselines, and Compliance

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/>

The Psychology of Security

Bruce Schneier

Security is both a feeling and a reality. And they're not the same. The reality of security is mathematical, based on the probability of different risks and the effectiveness of different countermeasures. We can calculate how secure your home is from burglary, based on such factors as the crime rate in the neighbourhood you live in and your door-locking habits. We can calculate how likely it is for you to be murdered, either on the streets by a stranger or in your home by a family member. Or how likely you are to be the victim of identity theft. Given a large enough set of statistics on criminal acts, it's not even hard; insurance companies do it all the time.

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

Fundamental Computer Investigation Guide for Windows

Microsoft

Internet connectivity and technological advances expose computers and computer networks to criminal activities such as unauthorized intrusion, financial fraud, and identity and intellectual property theft. Computers can be used to launch attacks against computer networks and destroy data. E-mail can be used to harass people, transmit sexually explicit images, and conduct other malicious activities. Such activities expose organizations to ethical, legal, and financial risks and often require them to conduct internal computer investigations.

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

PHP Security from the Inside

The Register

Stefan Esser is the founder of both the Hardened-PHP Project and the PHP Security Response Team (which he recently left). Federico Biancuzzi discussed with him how the PHP Security Response Team works, why he resigned from it, what features he plans to add to his own hardening patch, the interaction between Apache and PHP, the upcoming "Month of PHP bugs" initiative, and common mistakes in the design of well-known applications such as WordPress.

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

Guide to Computer Security Log Management

Nist.gov

A fundamental problem with log management that occurs in many organizations is effectively balancing a limited quantity of log management resources with a continuous supply of log data. Log generation and storage can be complicated by several factors, including a high number of log sources; inconsistent log content, formats, and timestamps among sources; and increasingly large volumes of log data. Log management also involves protecting the confidentiality, integrity, and availability of logs. Another problem with log management is ensuring that security, system, and network administrators regularly perform effective analysis of log data. This publication provides guidance for meeting these log management challenges.

Source: <http://csrc.nist.gov/>

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)

Trends in Malware Threats

Sophos

Ploys to steal information for financial gain look set to continue in 2007 with malware authors moving from large-scale to targeted, calculated attacks.

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

Organized malware factories threaten Internet users

IBM

Spam, malware, phishing, and other forms of cyberattacks will likely increase in 2007 as more cyber-criminals organize into sophisticated manufacturing and distribution networks that mirror in structure the computer industry's legitimate production channels, according to a study released Monday, January 29. The study, authored by IBM, warns of the emergence of a so-called "exploits-as-a service" industry.

Source: <http://www.iss.net/>

IPv4 Countdown Policy Proposal

APNIC

The exhaustion of IPv4 address is approaching round the corner. Geoff Huston's latest projection at Potaroo (as of January 6, 2007) (<http://www.potaroo.net/tools/ipv4/>) draws the date of IANA pool exhaustion as 31st May 2011, and that of RIR pool as 14th July 2012. Tony Hain projects similar dates based on a different algorithm of his own. From these data, we may observe that if that the current allocation trend continues, the exhaustion of IPv4 address space is expected to take place as early as within the next five years.

ICANN/IANA and RIRs must co-ordinate with stakeholders to achieve smooth termination of IPv4 address space as the Internet bodies responsible for stable management and distribution of IP number resources. This proposal provides some ideas as well as concrete examples of the policy that helps IPv4 allocations come to an end with "the minimum confusion" and in "as fair manner as possible".

Source: <http://www.apnic.net/>

Hardening Microsoft Windows – STIGS, Baselines, and Compliance

NIST.org

Windows hardening should be considered more of a prerequisite than an endpoint. But if you fall under any of the IT security compliance laws it is a very important prerequisite. As we say on our banner "It's not enough to be secure, you have to prove you're secure."TM

Windows hardening is basically locking down and securing the operating system. It involves removing unwanted services, configuring remaining services to operate with the least privilege necessary, disabling legacy support that isn't used, removing unused user accounts, enforcing a certain password complexity, closing unused open network ports, patching all known vulnerabilities, etc. All good stuff. If you fall under any of the various IT security compliance laws then hardening also involves a large degree of consistency and documentation.

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



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.