



AGAINST CYBER THREATS

CCIP e-Bulletin

CENTRE *for* CRITICAL INFRASTRUCTURE PROTECTION

Issue 39

Publication date: 16/05/07

Contents

- Coalition of Security Leaders Announces First Secure Coding Assessment and Certification Exams for Programmers
- CERT's Podcast Series: Security for Business Leaders
- Animated Cursor Security Bug
- How to Establish and Enforce a Wireless Security Policy
- Building A Web-Based Neighbourhood Watch
- Fraud: One of the Greatest Risks to a Company's Reputation & Viability
- Blended Threats Considerations
- NIST Issues Guidelines for Ensuring RFID Security
- Google Searches Web's Dark Side

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/>

Coalition of Security Leaders Announces First Secure Coding Assessment and Certification Exams for Programmers

SANS Software Security Institute

Governments, companies, and educational institutions are doomed to deal with endless streams of software vulnerabilities unless programmers learn to write much more secure code.

Several initiatives are underway to improve secure programming skills and knowledge. Symantec, Oracle, Microsoft, and a few other software companies are conducting short courses for their programmers; software firms like SPI Dynamics and Fortify Technology are working with universities to provide automated, real-time feedback to student programmers; and dozens of universities are creating elective courses on secure programming. Yet, even if all of those initiatives are successful, they are unlikely to affect even two percent of the existing 1.5 million programmers already in the work force or those who will be entering the work force over the next five years.

This paper describes a cooperative initiative involving 362 corporations, government agencies, and colleges that have put voice to the critical need for rapid improvement in secure programming knowledge and skills.

Source: <http://www.sans-ssi.org/>

CERT's Podcast Series: Security for Business Leaders

CERT/CC

Practicing strong computer security is a nonnegotiable requirement for organizations doing business today. However, building security into an existing corporate culture is a complex undertaking. This series of podcasts provides both general principles and specific starting points for business leaders who want to launch an enterprise-wide security effort or make sure their existing security program is as good as it can be.

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

Animated Cursor Security Bug

Microsoft

A core tenet of the SDL is to take and incorporate lessons learned when we issue a security update, and there is a great deal to learn from the recent animated cursor bug, MS07-017, so I want to spend a few minutes to go over some of the things we have learned from this bug.

Source: <http://blogs.msdn.com/>

How to Establish and Enforce a Wireless Security Policy

Security Park

All security starts with a policy – of what behaviours we will allow and which are prohibited. With the rapid growth and market adoption of wireless products, and the unfortunate growth in computer security threats and attacks, every enterprise (no matter what size) should have a wireless security policy.

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

Information Security Links

Centre for the Protection of National Infrastructure (CPNI)

Canadian Cyber Incident Response Centre (CCIRC)

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)

Building A Web-Based Neighbourhood Watch

Security Fix

At any given time, tens of millions of personal computers around the globe are infected with malicious software that criminals use to turn them into spam-relaying “zombies.” But many machines could be inoculated if there was a distributed, Internet-wide system for notifying Web surfers that their machines were being used to defraud and attack others online.

Source: <http://blog.washingtonpost.com/>

Fraud: One of the Greatest Risks to a Company's Reputation & Viability

KPMG

Hard on the heels of its 2006 Fraud Survey, KPMG has released a white paper to help organisations develop a strategy to prevent, detect and respond to corporate fraud.

The KPMG Fraud Survey revealed that more than 50 per cent of New Zealand businesses continue to be the victims of fraud and the number of employees with a history of dishonesty has doubled since the last survey.

Source: <http://www.kpmg.co.nz/>

Blended Threats Considerations

Paul A. Henry

According to SANS, every 24 minutes an Internet-facing network comes under some form of attack; this is not apocalyptic marketing spin, this is a fact of life for today's Internet. The sheer volume of threats along with the continued evolution of application layer threats and the increasing dominance of blended threats require that we re-evaluate our current defensive architectures.

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

NIST Issues Guidelines for Ensuring RFID Security

US National Institute of Standards and Technology

Retailers, manufacturers, hospitals, federal agencies and other organizations planning to use radio frequency identification (RFID) technology to improve their operations should also systematically evaluate the possible security and privacy risks and use best practices to mitigate them, according to a report* issued today by the National Institute of Standards and Technology (NIST).

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

Google Searches Web's Dark Side

BBC

One in 10 web pages scrutinised by search giant Google contained malicious code that could infect a user's PC. Researchers from the firm surveyed billions of sites, subjecting 4.5 million pages to “in-depth analysis”. About 450,000 were capable of launching so-called “drive-by downloads”, sites that install malicious code, such as spyware, without a user's knowledge.

Source: <http://news.bbc.co.uk/>



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.