

Issue 88

Publication date: 04/11/2009

Contents

- Clearinghouse for Incident Handling Tools
- Mitigation Monday #2 - Defense against Drive-By Downloads
- Secure Design Patterns
- Small Business Information Security: The Fundamentals
- The "Korean" Cyber Attacks and their Implications for Cyber Conflict
- Why Security Matters NOW
- Announcing the Release of the Enhanced Mitigation Evaluation Toolkit
- Cybercriminals Use Fear and Anxiety to Convince Users to Buy Rogue Security Software
- Aligning Network Security with Business Priorities

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/>

Clearinghouse for Incident Handling Tools

European Network and information Security Agency (ENISA)

This is a pilot site for a proposed collection of tools and guidelines of their use intended for incident handling teams. Information on this site reflects the experience of a number of European CSIRTs, working together as a project in the framework of the TERENA's Task Force TF-CSIRT. By this the project likes to create a repository of information about tools that are actively used and supported by active CSIRTs.

Source: <http://www.enisa.europa.eu/>

Mitigation Monday #2 - Defense against Drive-By Downloads

National Security Agency

Every network that contains important defense, political, or economic information is a target. These networks contain information representing billions of dollars in research and years of technical advantage. When military secrets are stolen, our troops face harm from adversaries who know too much. When economic data is stolen, our adversaries gain advantage over us in trade negotiations. When engineering designs are stolen, our adversaries can replicate or improve them—a resolute adversary could even modify our designs to make them malfunction at key moments. Many CIOs are unaware of how vulnerable their networks are and how aggressively they are being targeted. This mitigation report presents a common attack scenario for Microsoft Windows networks and discusses how it can be prevented using a defense-in-depth strategy.

Source: <http://www.nsa.gov/> (pdf)

Secure Design Patterns

CERT/CC

This report describes a set of secure design patterns, which are descriptions or templates describing a general solution to a security problem that can be applied in many different situations. Rather than focus on the implementation of specific security mechanisms, the secure design patterns detailed in this report are meant to eliminate the accidental insertion of vulnerabilities into code or to mitigate the consequences of vulnerabilities. The patterns were derived by generalizing existing best security design practices and by extending existing design patterns with security-specific functionality. They are categorized according to their level of abstraction: architecture, design, or implementation.

Source: <http://www.cert.org/> (pdf)

Small Business Information Security: The Fundamentals

NIST

NIST Computer Security Division announces that NISTIR 7621, Small Business Information Security: The Fundamentals, has been released. NISTIR 7621 is intended to help small businesses and small organizations implement the fundamental components of an effective information security program.

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

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

CCIP Security Guidelines

NetSafe

National Cyber Alert System (USA)

AusCERT National Information Technology Alert Service (AUS)

IT Security Awareness For Everyone (UK)

National Alerting Service (Netherlands)

The “Korean” Cyber Attacks and their Implications for Cyber Conflict

Center for Strategic and International Studies

It has been several months since the basic “denial of service” attacks against networks in the United States and South Korea in early July. No one has yet taken credit, nor have others been able to determine the attackers’ identity. As with many other cyber incidents, there is no conclusive evidence as to who was responsible.

Source: <http://csis.org/>

Why Security Matters NOW

CIO Magazine

Social networking and cloud computing threats abound, making information security important once again to business leaders, reports the annual Global Information Security Survey. Find out the direction of security spend, and the nature and impact of the new wave of cyber outlaws.

Source: <http://cio.co.nz/>

Announcing the Release of the Enhanced Mitigation Evaluation Toolkit

Microsoft

Even as you read this, people around the world are hunting for vulnerabilities in software applications. Odds are some of them will be successful. Depending on their motives and what they find, your software and systems may be put at risk. So how do you protect your software from unknown vulnerabilities that may or may not exist? One option is to use security mitigations.

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

Cybercriminals Use Fear and Anxiety to Convince Users to Buy Rogue Security Software

Symantec

Symantec Corp. announced the findings of its Report on Rogue Security Software. The study’s findings, based on data obtained during the 12-month period of July 2008 to June 2009, reveal that cybercriminals are employing increasingly persuasive online scare tactics to convince users to purchase rogue security software. Rogue security software, or “scareware,” is software that pretends to be legitimate security software. These rogue applications provide little or no value and may even install malicious code or reduce the overall security of the computer.

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

Aligning Network Security with Business Priorities

SearchSecurity

Network security experts know that executives expect them to be familiar with firewall rulesets and capable of spotting potential network intrusions. What fewer of them realize, however, is that the network, like the rest of the organization, must be aligned with the enterprise’s business priorities. This tip will discuss ways to align the day-to-day network security operations of an organization with its business problems and priorities.

Source: <http://searchsecurity.techtarget.com/>



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.

