

Issue 86

Publication date: 23/09/2009

Contents

- How to Measure Security? NIST Maps out the Emerging Field of IT Metrology
- Truth, Lies and Fiction about Encryption
- ENISA launches Guide on sharing information to mitigate network security vulnerabilities, threats and cyber attacks
- CERT's Podcast Series: Security for Business Leaders
- Seven Reasons Websites are not Secure
- State of Internet Security, Q1-Q2 2009
- Who Put the IPv6 in my Internet?
- Gartner Outlines Four Risk Management Mistakes that Could Threaten Security Budgets
- Control System Scanning with Nessus: Part 1

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/>

How to Measure Security? NIST Maps out the Emerging Field of IT Metrology

GCN

Information technology security is a hot topic, but attention usually focuses on the lack of it. What is missing is an objective, quantifiable way to effectively measure it. "Security can be looked at in different ways by different people," said Wayne Jansen, a computer scientist at the National Institute of Standards and Technology's IT Laboratory. There is quality control for code developers, the process of deploying a system, and its maintenance by users. "These are all different aspects," and they do not lend themselves to traditional methods of measurement used in physical science, he said. Jansen has examined the status of efforts to develop security metrics, identified challenges and suggested a course for future research in a recent NIST report, "Directions in Security Metrics Research."

Source: <http://gcn.com/>

Truth, Lies and Fiction about Encryption

SearchSecurity

It's a security practitioners dream to deploy a technology that ensures perfect data protection 100 percent of the time. Short of unplugging a computer and locking it in a vault, few technologies come as close as encryption to nearly unbreakable data security; take the data, run it through an encryption algorithm, and it's unreadable to anyone who doesn't possess the right key to reverse the process. It can be mathematically demonstrated that retrieval of encrypted data without the encryption keys is computationally impossible within the expected lifetime of the universe.

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

ENISA launches Guide on sharing information to mitigate network security vulnerabilities, threats and cyber attacks

European Network and Information Security Agency

EU Agency ENISA presents the first pan European Good Practice Guide on Network Security Information Exchange (NSIE). The main aim of this guide is to assist Member States and private stakeholders in setting up and running NSIEs at national level. The guide could also pave the way for the creation of the first pan European NSIE for critical communication networks and services.

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

CERT's Podcast Series: Security for Business Leaders

CERT®

Practicing strong information and cyber 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/>

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)

Seven Reasons Websites are not Secure

TechWorld

Conventional wisdom is that Web wanderers are safe as long as they avoid sites that serve up pornography, stock tips, games and the like. But according to recently gathered research from security firm Sophos, sites we take for granted are not as secure as they appear.

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

State of Internet Security, Q1-Q2 2009

Websense

Today, Websense released its biannual "State of the Internet" report, a deep dive into the most significant threats on the Internet during the first half of 2009. Today, most threats to information security are leading to the Web -- either using the Internet as the attack vector, or simply the route through which stolen, confidential data is transmitted.

Source: <http://securitylabs.websense.com/>

Who Put the IPv6 in my Internet?

Arbor Networks

About this time last year, we released a study on the state of IPv6 deployment in the Internet. Our August 2008 paper found diminishingly small traces of IPv6 — less than one hundredth of 1% of Internet traffic. This year? In a dramatic reversal of long-term IPv6 stagnation, global IPv6 traffic globally grew more than 1,400% in the last 12 months. Even more remarkable, this growth is due primarily to one application and one ISP.

Source: <http://asert.arbornetworks.com/>

Gartner Outlines Four Risk Management Mistakes that Could Threaten Security Budgets

DarkReading

Enterprise security budgets have always been difficult to justify, and the global economic crisis is making this critical process even more difficult, according to Gartner, Inc. Corporate security professionals face a complex situation as they work with highly constrained financial and staffing resources to manage and mitigate a rapidly changing and expanding risk environment.

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

Control System Scanning with Nessus: Part 1

Digital Bond

A few weeks back while discussing some planned Nessus updates and Bandolier, I said what matters is value and improved security for your control systems, not just running a scan. There are a variety of reasons why you might want to scan your control networks but suffice it to say that you should be scanning with a goal in mind, not just scanning for the sake of scanning. Perhaps you want to identify known vulnerabilities, audit security configuration, or check patch levels. Whatever your goal is, it's worth taking a look at the Nessus configuration and planning your scans according to that goal.

Source: <http://www.digitalbond.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.

