CERT'S PODCASTS: SECURITY FOR BUSINESS LEADERS: SHOW NOTES

Tackling Tough Challenges: Insights from CERT's Director Rich Pethia

Key Message: Rich Pethia reflects on CERT's 20-year history and discusses how he is positioning the program to tackle future IT and security challenges.

Executive Summary

CERT's vision is a securely connected world. CERT's mission is to enable informed trust and confidence in the use of information technology. To achieve this vision and mission, CERT has broadened its perspective to include the full system/software engineering and operations life cycle and is reaching out to thought leaders in the global IT and security community.

In this podcast, Rich Pethia, director of the CERT Program at Carnegie Mellon University's Software Engineering Institute, discusses the past, current, and future state of Internet security and CERT's role in tackling future challenges as CERT celebrates its 20th anniversary.

PART 1: LOOKING BACK, LOOKING FORWARD: THE GOOD, THE BAD, AND THE UGLY

CERT's Vantage Point

CERT's vision is a securely connected world, supported by CERT's mission of enabling informed trust and confidence in the use of information technology.

As the director of CERT, Pethia has unique access to government, commercial, and industry leaders.

The Good News

Internet use continues to grow, not just in size (number of people, volume of traffic) but also in utility, for example:

- the increasing amount of real government and business operations
- the introduction of new applications
- the growing use of new mobile appliances

User awareness of the need to address security is increasing along with increasing attention from service providers (firewalls, virus protection, anti-spyware, data backup).

Developers are paying more attention to building security into their products. Vendors have more mature processes for providing cost-effective, timely updates for software vulnerabilities.

Users are more willing to report cyber crimes and law enforcement is becoming more effective in prosecuting criminals.

The Bad and The Ugly

The sophistication level of capabilities and activities of the bad guys is growing, especially over the last couple of years.

Cyber criminals have moved from mischief makers and vandals to smart, sophisticated, cause-motivated, for profit crimes.

Criminals are able to purchase or rent botnets to launch a denial-of-service attack or spam. For-hire cyber mercenaries will gladly write custom-tailored viruses with money-backed guarantees. Pirated credit card and personal ID information are available for purchase.

Organized crime is growing and poses a significant current and future threat.

The Need for Comprehensive, Continuous Risk Management

Business leaders often implement a specific technology or adopt a "check the box" practices program to meet specific compliance obligations.

These types of approaches provide limited value given frequent changes in threats and vulnerabilities.

Continuous risk management is a much more effective and sustainable approach.

Information leakage and exposure will occur given criminal motivations and the changes in our use of computing technology (for example, social networking, lower privacy barriers, and mobile computing).

Outsourced IT operations and cloud computing increase risk.

PART 2: CERT'S EVOLUTION: THE SYSTEM LIFE CYCLE

Positioning CERT

To better address the fundamental issues of software and system assurance, Rich has broadened the scope of the CERT Program in several significant ways.

Today's projects address security issues across the engineering and operations lifecycle, such as:

- building security into complex systems and networks
- improving coding practices to reduce vulnerabilities in newly deployed software
- better system and network monitoring to detect problems earlier
- more effective analysis of security event data produced by security technologies
- helping users and organizations understand what a comprehensive security program looks like
- better threat identification and detection
- dealing with issues of scale for intrusions that can involve thousands of computers and terabytes of data
- ways to improve workforce skills and knowledge

Dealing with Growing Complexity

Organizations responsible for providing IT products and services to their users need to:

- take a holistic approach
- understand computing and security technology
- understand their own policies and practices, and their intent
- pay attention to building workforce skills to help staff avoid mistakes
- maintain constant vigilance and awareness of the threat landscape
- do the above in a continuous way

In parallel, a piecemeal approach helps in identifying solutions for specific problems.

One example is CERT's work with law enforcement when conducting forensic examinations of computing hardware and software – both those used in committing a crime and those that are targets of a crime.

PART 3: BROADENING CERT'S RESEARCH AGENDA; WORKING WITH CERT

Outreach Initiatives

Given its FFRDC status, CERT works closely with the U.S. Department of Defense and the U. S. Department of Homeland Security.

That said, CERT also looks across the broader IT landscape, both nationally and globally. Today, almost all government and business operations have an international component.

For the last year, CERT has conducted a Distinguished Speaker Seminar Series in concert with Carnegie Mellon's CyLab. Executives and thought leaders in information technology and security are invited to share their perspective and ideas regarding pervasive issues and promising solutions.

Some of the topics that have come from this series include issues surrounding controls systems, mobile computing, and social computing.

In March 2009, CERT is hosting a two-day technical symposium titled "Security Challenges in an Evolving World." Invited speakers have either very broad or very deep perspectives on future security and computing issues.

CERT's objective is to better understand where the technology is headed, how network use may change over time, and what may occur in the policy and regulation space. The intent is to better anticipate future problems and promising solutions.

Accessing CERT's Work

Much of CERT's work is publicly available on the CERT web site. This includes a wide range of publications, podcasts, and training.

Through the SEI Affiliates Program, organizations can send a staff member to work at the SEI for a period of time. In addition, CERT often works directly with organizations on specific projects.

One example is CERT's work with the Financial Service Technology Consortium to develop the Resiliency Engineering Framework, a comprehensive process model that integrates security, IT, and business continuity.

CERT is always looking for new ways to work with people on tough problems.

Resources

Pethia: InfoSec's Challenges, Changes