CERT PODCASTS: SECURITY FOR BUSINESS LEADERS: SHOW NOTES

CERT Lessons Learned: A Conversation with Rich Pethia, Director of CERT

Key Message: This podcast discusses CERT's history and lessons learned that can help organizations and their Computer Security Incident Response Teams (CSIRTs) be successful.

Executive Summary

CERT is a center of Internet security expertise, located at the Software Engineering Institute, a federally funded research and development center operated by Carnegie Mellon University. CERT studies Internet security vulnerabilities, researches long-term changes in networked systems, and develops information and training to help organizations improve security.

While CERT continues to respond to major security incidents and analyze product vulnerabilities, CERT's role has expanded over the years. Along with the rapid increase in the size of the internet and its use for critical functions, there have been progressive changes in intruder techniques, increased amounts of damage, increased difficulty of detecting an attack, and increased difficulty of catching the attackers.

The CERT Program's primary goals are to ensure that appropriate technology and systems management practices are used to resist attacks on networked systems and to limit damage and ensure continuity of critical services in spite of successful attacks, accidents, or failures ("survivability").

This conversation with Rich Pethia, the director of CERT, briefly describes CERT's history and several of the key lessons learned that can assist other organizations in creating an effective security incident response capability. Rich also challenges technology producers, service providers, system administrators, and business leaders to recognize their role in contributing to more robust Internet security.

PART 1: CERT HISTORY

Background

Following the Morris Worm incident, which brought 10 percent of Internet systems to a halt in November 1988, the Defense Advanced Research Projects Agency (DARPA) charged the SEI with setting up a center to coordinate communication among experts during security emergencies and to help prevent future incidents. This center was named the CERT Coordination Center (CERT/CC).

At that time, the Internet was called the ARPANET, had approximately 200,000 systems connected to it, and served primarily as an open research network for academic and other research institutions. The ARPANET itself was a research project in survivable networks.

DARPA issued a press release announcing the creation of CERT on December 7, 1988. The first call came in that evening from a U.S. government lab being attacked from outside of the U.S. Investigators weren't sure what to do, so CERT was able to assist in tracking down the source of the attack and helped the attacked and attacking sites to correct the problem.

Early, Key Decisions

CERT will

- be a service organization with success measured by delivering value to Internet users. CERT has no authority to

direct or control anyone's actions.
- build on CMU's and SEI's strengths and core competencies -- focus on
  - resolving technical and software issues
  - understanding exploited vulnerabilities
  - diagnosing the extent of security incidents (how many systems are compromised and how deeply systems are affected)
  - providing technical advice on how to repair systems and restore operations
- take extreme care to protect sensitive information
  - that belongs to the organizations contacting CERT (identity, mission, system configurations, vulnerabilities, nature of the attack, etc.)
  - as part of ongoing investigations, including not disclosing the fact that an investigation is underway
- serve as a model to help other organizations build their own incident response capabilities at the corporate and national levels (refer to Forum of Incident Response and Security Teams (FIRST)

Building and protecting the trust that is placed in CERT by the community it serves is one of the most important keys to success.

The CERT Charter

CERT is chartered to work with the internet community in detecting and resolving computer security incidents, as well as taking steps to prevent future incidents. In particular, our mission is to

- Provide a reliable, trusted, 24-hour, single point of contact for emergencies.
- Facilitate communication among experts working to solve security problems.
- Serve as a central point for identifying and correcting vulnerabilities in computer systems.
- Maintain close ties with research activities, and conduct research to improve the security of existing systems.
- Initiate proactive measures to increase awareness and understanding of information security and computer security issues throughout the community of network users and service providers.

PART 2: CERT TODAY; AVAILABLE RESOURCES

Evolving Mission

CERT's mission and services have evolved, building upon the foundation of operational incident response and CERT's breadth and depth of understanding based on the thousands of reports that CERT receives.

By abstracting information, CERT is able to describe

- generic attack styles and patterns
- how attack technology is evolving
- weaknesses in particular products

without identifying any individual organization or systems.

The attacker, threat, vulnerability, technology, and security solution landscape is constantly changing. Today's solutions will likely not be sufficient tomorrow. Computer Security Incident Response Teams (CSIRTs) perform a critical service in keeping their using communities up to date.

Observed State of Practice

Through experience, CERT gained in-depth understanding about software vulnerabilities, how systems were being used and attacked, the increased use of automation, and how attackers were using the Internet itself to launch attacks on connected systems.

CERT observed that many organizations do not understand how to put basic security policies and practices in place. CERT wasn't seeing, for example, 500 different kinds of incidents, but rather was seeing the same incident repeating 500 times.

Useful Resources

Initially, CERT developed simple guidelines (tech tips) that organization can use to put useful security practices in place. These have evolved into robust courseware and curricula. Handbooks, textbooks, and CERT's Virtual Training Environment are also available.

PART 3: PROGRESS AND PROMISING SOLUTIONS

Scope and Breadth of Security Landscape Expanding

Security needs to be addressed across the entire system and software life cycle. And a growing list of roles needs to be considered, all of whom play a part:

- technology and software producers
- service providers (IT, Internet)
- users of information technology (large to small organizations)
- individual users, both in businesses and at home

For all roles, it is important to remember that when you are connected to the Internet, the Internet is connected to you.

Technology Producers

Technology producers need to understand that they are releasing products into a hostile environment, and these products will be attacked. Producers need to focus on:

- developing more secure products that can withstand attack and emerging threats
- higher quality implementations (for example, eliminate the ever-present buffer overflow)
- the fact that it is much more cost effective to find problems in development, not after the product has been deployed. Correcting problems after the fact is very expensive.
- providing user interfaces that are simple enough for the average user to use without requiring deep understanding of the underlying technology

Service Providers

Service providers need to continue to expand the security services they provide for their customers (anti-virus, firewalls, etc.).

System Administrators; An Enterprise-Wide Approach

System operators and their management chain need to understand that sustainable security requires an enterprise-wide approach:

- to deal with the constantly changing threat
- to ensure everyone knows the organization's policies and their role
- to set up and manage accounts in a secure manner
- to protect information which the organization owns and for which it is the custodian (customer, partners, employees)
- to report security problems in a timely manner and know who to inform

---

SECTION 4: WHAT SHOULD LEADERS DO?

- Demonstrate visible commitment and support for enterprise-wide security, including living by the organization's policies (for example, not sharing account information with administrative staff so they can handle email). Walk the talk.
- Provide IT staff with the time necessary to understand what effective security policy and practice look like; time to build staff skills and competencies.
- Ensure the security budget is adequate.
- Make sure that policies and practices are enforced; no special cases.
- Security left unattended degrades. Leaders need to treat security as a requirement of being in business, requiring continuous monitoring and improvement.
- Integrate security into the day-to-day processes of the organization.
- Recognize that this problem is not going away.
- Take advantage of the publications and guidance available on the SEI and CERT web sites.
- Take advantage of FIRST (Forum of Incident Response and Security Teams) -- the worldwide network of more than 200 incident response teams.

References

"Meet CERT." http://www.cert.org/meet_cert/meetcertcc.html
