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

Establishing a National Computer Security Incident Response Team (CSIRT)

Key Message: A national CSIRT is essential for protecting national and economic security, and ensuring the continuity of government agencies and critical infrastructures.

Executive Summary

A national CSIRT manages incidents that have national significance (those involving crime, espionage, economic interests, and terrorism). In addition, it builds awareness and advocacy for safe, secure, and intelligent use of the internet and other information and communication technologies (ICT). Establishing a national computer security incident response (CSIRT) capability involves planning, building stakeholder sponsorship, building trust, managing incidents, and helping form a national cyber security strategy.

In this podcast, John Haller, a member of the CERT Resilience Enterprise Management team, and Jeff Carpenter, a member of the CERT Coordination Center, discuss the goals and actions necessary to create a computer security incident response team (CSIRT) at the national level.

PART 1: THE ROLE OF A NATIONAL CSIRT

Why Create a National CSIRT?

The focus of a national CSIRT, from a cyber perspective, is to protect

- national and economic security
- the ongoing operations of a government
- the ability of critical infrastructures to continue to function

A national CSIRT

- monitors incidents at a national level
- identifies incidents that could affect critical infrastructures, defense, and the economy
- warns critical stakeholders and the nation about computer security threats
- helps build organizational CSIRTs in the public and private sectors

Components of critical infrastructures are often held by private sector organizations. A national CSIRT reaches out to such organizations to help identify and resolve issues in the national interest.

The Mission of a National CSIRT

A national CSIRT responds to incidents that have national significance – those involving crime, espionage, economic espionage, and terrorism.

National CSIRTs need to build capabilities to perform the following activities:

- Receive incident information.
- Analyze information to determine if an incident is nationally significant.
- Correlate information from multiple sources to get a complete picture.
- Provide advice to government and critical infrastructure stakeholders on how to protect and define their networks and, when compromised, how to recover.

- Serve as the international point of contact for their country in the event of an international incident.
- Collaborate with national law enforcement, intelligence, government, and critical infrastructure organizations.
- Help organize and conduct national exercises for responding to incidents of national significance.

Four Strategic Goals for a National CSIRT

These are as follows:

- Goal 1 – Plan and establish a security incident management capability.
- Goal 2 – Establish situational awareness.
- Goal 3 – Manage cyber incidents.
- Goal 4 – Support the national cyber security strategy.

PART 2: GOAL 1 – PLAN AND ESTABLISH A CSIRT CAPABILITY

Engage Stakeholders; Understand Constraints

Those planning for a national CSIRT need to make sure that the expectations of government and industry are aligned with respect to national CSIRT roles, responsibilities, services, and operations.

Constraints to consider include staff capabilities and funding.

Where Should the CSIRT Reside/Report?

Planners need to determine if the national CSIRT should be housed within government, reside in the private sector, or reflect a combination of both.

Due to the increased attention on national and economic security, governments are realizing that certain CSIRT functions need to be within the government.

Government agencies that often serve as the organizational home for a national CSIRT include

- commerce department or ministry
- telecommunications regulatory agency
- interior department or ministry
- a legal entity such as an attorney general department

Authority of the National CSIRT

During the planning activity, participants need to determine and define the authority of the national CSIRT. The scope of authority may include

- authority over government operations and use of information technology
- authority over the public’s use of the internet

Most national CSIRTs function best in an advisory capacity, not in a regulatory or authority role.

PART 3: GOALS 2, 3 – BUILD SITUATIONAL AWARENESS; MANAGE INCIDENTS

Build Trust

The key for a national CSIRT to become situationally aware with regard to emerging and significant incidents is trust. Organizations that are providing information to a national CSIRT need to be confident that their information will be adequately protected.

Establishing trust comes from good personal relationships between leaders and good policies and procedures for protecting information.

A national CSIRT needs to obtain accurate information so that it can provide the right guidance to the right stakeholders so that they can respond to incidents and mitigate damage.

Recognize the Dual Role of the CSIRT

A national CSIRT should focus on incidents of national significance. That said, when it first starts providing services, it often can be inundated with all types of requests. The CSIRT needs to be able to deal with this effectively.

A national CSIRT's primary responsibility is to protect critical infrastructures. But a national CSIRT is also responsible for warning and advising the public on how to use the internet in a more safe and secure manner.

Operational Capabilities

A national CSIRT needs to be able to

- accept incident information (have an effective intake mechanism)
- let the public know about vulnerabilities and problems (provide national alert and warning services)
- communicate best practices and lessons learned from incidents including steps people can take to protect themselves
- analyze incidents
- inform stakeholders regarding the meaning of an incident

Use Existing National CSIRTs as a Resource

Those planning a new national CSIRT should take full advantage of the wealth of resources from national CSIRTs that have been in business for some time. These resources can be accessed on the CERT website.

PART 4: GOAL 4 – SUPPORT THE NATIONAL CYBER SECURITY STRATEGY

In the Absence of a National Cyber Security Strategy

Often, a national CSIRT develops in parallel with (or in the absence of) a national cyber security strategy. One activity often informs the other and vice versa.

To get started, members of the national CSIRT should

- talk to key government stakeholders early and often
- educate stakeholders about the importance of cyber security and the extent to which critical infrastructures are dependent upon information and communications technology (ICT)

In the Presence of a National Cyber Security Strategy

If there is a national strategy, members of a national CSIRT should

- help government stakeholders understand cyber security from a policy and legislative perspective
- convey how cyber security affects what the government does (regulation, use and purchase of information systems, etc.)
- help government agencies partner with private sector organizations including critical infrastructure providers
- help organizations in both the public and private sector build their own CSIRTs

Identify a Sponsor for a National CSIRT

Champions or sponsors of a national CSIRT typically are one of the following:

- a government agency leader with a technology management responsibility including infrastructure to protect
- an academic leader who is focused on technology and/or security and serves as an advocate to the government

First Steps for Getting Started

The following steps are useful to start a national CSIRT:

- Talk with other national CSIRTs and participate in national incident management forums.
- Determine your constraints and develop a realistic picture of what you can do.
- Talk with key stakeholders in government agencies and critical infrastructure provider organizations.

Resources

Best Practices for National Cyber Security: Building a National Computer Security Incident Management Capability

CERT National CSIRT web page

European Network and Information Security Agency (ENISA)

Forum of Incident Response and Security Teams (FIRST)

Asia Pacific CERT (APCERT)

CERT podcast: Managing Risk to Critical Infrastructures at the National Level

CERT podcast: Tackling Security at the National Level: A Resource for Leaders