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

Tackling Security at the National Level: A Resource for Leaders

Key Message: Business leaders can use national CSIRTs (Computer Security Incident Response Teams) as a key resource when dealing with incidents with a national or worldwide scope.

Executive Summary

Not all information security incidents can be handled in-house. Some require coordination with third-party forensics firms or law enforcement personnel, others with external partners or suppliers, and still others with national or global organizations. In these latter types of incidents, the expertise of a national CSIRT (Computer Security Incident Response Team) can be a valuable resource for business leaders.

National CSIRTs deal with security at the macro level. They focus on large-scale incidents or incidents that can affect the economy, critical infrastructure, government operations, or national security. If they are dealing with a worldwide event, they can coordinate with national CSIRTs in other countries to establish communications and cooperation among those countries to deal with the incident.

In this podcast, Jeff Carpenter, the technical manager of the CERT Coordination Center, discusses how national CSIRTs work and how business leaders can make use of national CSIRTs' expertise to handle large-scale, critical situations as smoothly as possible.

PART 1: AN INTRODUCTION TO NATIONAL CSIRTS

What Do National CSIRTs Do?

Two definitions:

CSIRT (Computer Security Incident Response Team) – a team within an organization that helps address and coordinate computer security incident response issues.

National CSIRT – a team that helps address large-scale and/or critical computer security incidents affecting one or more countries.

Critical computer security incidents may affect:

- The economy
- Critical infrastructure
- Government operations
- National security

By nature, these types of incidents usually affect many organizations, rather than just one.

National CSIRTs also are interested in:

- Activity in their own country that can have an impact in other countries
- Activity in other countries that can have an impact in their own country

Growing the National CSIRT Base

Worldwide, there are between 30 and 50 national CSIRTs in various stages of maturity. Most are in the Americas, Asia, and Europe, and a few have recently been established in the Middle East. The United States' national CSIRT is called US-CERT.

Generally, it is in the interest of all national CSIRTs for more national CSIRTs to be established.

There are several reasons for this

- Increased ability to stop attacks or engage law enforcement around the globe
- Increased ability to educate more people in more countries about what to do to protect themselves on the Internet
- Increased ability to identify and neutralize malicious activity earlier, at its origin, before it cascades

---

PART 2: HOW BUSINESS LEADERS CAN INTERACT WITH NATIONAL CSIRTS

An Information Conduit

Why would a business leader want to use a national CSIRT's capabilities?

The national CSIRT may have access to information that the business does not, related to:

- the overall scope of the threat
- whether specific industries or companies are targets
- technical vulnerabilities that an organization might need to address within its infrastructure

This is especially true if the organization is in a critical infrastructure sector upon which the government is highly dependent such as telecommunications or financial services.

In these cases, it's in the government's interest to work with industry and help them understand what the risks and threats are, in advance of a problem or incident.

Finding a National CSIRT

Proactive is better than reactive in establishing a relationship with a national CSIRT – minimizing the potential for compromise of critical infrastructure, versus reacting to it after it's already happened.

To find out if your country has a national CSIRT, consult the national CSIRT list on the CERT website.

If none is listed, a national CSIRT still may be in the process of forming in your country. Try contacting national law enforcement, the national telecommunications regulation authority, or a government ministry that oversees Internet service providers. They may know about any national CSIRT efforts in the country.

This is not to say contacting a national CSIRT is the same as contacting law enforcement. It is not.

> **Law enforcement focus**: finding out who committed a crime and working to get them arrested
>
> **National CSIRT focus**: finding out how an incident happened, what methods and techniques were used, and working to prevent it from happening again – by mobilizing the community or a particular industry, if necessary

Establishing a Trust Relationship

If a national CSIRT exists in your country, what is the best way to establish a relationship?

In several countries, the national CSIRT comes together with business leaders in an advisory capacity to share and discuss issues and, most importantly, **develop a trust relationship**.

Trust is key because of the sensitive nature of the data an organization may share with a national CSIRT.

In fact, before sharing any issues or vulnerabilities with their national CSIRT, business leaders should:

- Discuss their intentions with legal counsel. Some laws and regulations may prohibit or discourage business leaders from providing certain information to a national CSIRT. For example, if the national CSIRT is considered a government entity, information disclosed to it may be accessible via an open records law.

  HOWEVER: Business leaders may not need to reveal every detail and aspect of an incident to get assistance. There may be no need to state which particular asset was compromised, for example, or who was affected.

- Also, information sensitivity may decrease over time – so the benefit of providing information today to get help may outweigh the potential cost of disclosure three years from now.

- Lastly, many national CSIRTs have policies protecting the confidentiality of information submitted to them. Don't assume this, however – check with your legal counsel regarding the laws in your particular country.

Business leaders can use their national CSIRT to help interface with local vendors in other countries. For example, US-CERT interacts with JP-CERT (Japan) as a faster, more effective interface with Japanese software vendors, rather than going to the vendor directly.

PART 3: HOW NATIONAL CSIRTS WORK IN TANDEM

Gauging Success by Silence

National CSIRTs' greatest moments generally are not the high-profile events that make it into the media.

Instead, they are the events that never occurred because national CSIRTs worked together to stop them.

In the middle of chaos, such as with the Code Red outbreak, national CSIRTs, vendors, and law enforcement all are trying frantically to communicate around the globe, and this does not always work perfectly.

However, in a calmer environment before a major security problem evolves from theory to practice, a problem-solving process among national CSIRTs may look like this:

- What's the technical solution to solve this vulnerability?
- Who is likely to be significantly impacted?
- How do we get information to the right people to make the changes that need to be made?
- Are there workarounds that can be deployed prior to the vendor developing a solution?

All of this goes on behind the scenes, and many times the problem is solved before it surfaces.

Divide, Share, and Conquer

Additionally, national CSIRTs tend to focus and coordinate their efforts, because it is impractical for every CSIRT to do everything. For example:

- The Brazilian national CSIRT has developed a specialty in honeypots.

- The South Korean national CSIRT has developed a specialty in identifying real-time threats on backbone Internet service providers.

In these and many other cases, specialty knowledge can be shared with other national CSIRTs, thereby strengthening the world community and avoiding duplication of effort.

Resources

National CSIRTs list

National CSIRTs portal