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

The Real Secrets of Incident Management

Key Message: Incident management is not just about technical response. It is a cross-enterprise effort that requires good communication and informed risk management.

Executive Summary

The term "computer security incident response team" may call to mind images of IT personnel scrambling to reload downed servers with backups. But a CSIRT (computer security incident response team) cannot be made up solely of technical personnel. Many people in many departments across the organization must be involved, and all employees must be aware of two things: 1.) the organization's definition of "incident"; and 2.) who to contact if an incident occurs.

In this podcast, Georgia Killcrece and Robin Ruefle, the leaders of CERT's CSIRT development team, discuss lessons learned. Specifically, they focus on the importance of good communication and defined workflows for successful incident management.

PART 1: COMMUNICATION IS KEY

Even the best-defended network can still suffer attacks, so an effective incident management capability is needed. How can an organization achieve this?

First, some quick definitions: An event can be viewed as any kind of "anomalous activity" on a network.

Some events qualify as incidents. Different types of organizations may have different definitions of "incident"--but everyone within a particular organization should agree on that organization's definition!

What do you need for good incident management?

- Be proactive; just reacting to an event is not enough.
- Look at end-to-end activities and interdependencies across the organization, those involving many departments rather than just the IT department
- Find ways to foster good communication among these various departments

Good communication starts with employees in the trenches:

- Do they understand what is malicious and what is not?
- Who do they contact if they believe an incident has occurred?
- What is the process or workflow from that initial contact to the experts who are responsible for analyzing a given type of incident?

Here's an example of the importance of good communication. Several recent state laws require organizations to report disclosures of personal information. However, if the appropriate people don't know a disclosure has happened or if employees don't know what to do if they believe a disclosure has occurred, the right people might not find out. The organization might find itself unable to comply with the law and thus legally liable.

In general, if information is not getting to the right people and places within the organization, you could be missing a lot that could damage your organization, and your reputation.

Therefore, everyone needs to understand when and how to pass on information and to whom to pass it.

Keep in mind that "incident response" is not just technical; it's also managerial and administrative and may involve, among others:

- Human resources
- Public relations
- Legal counsel

Also keep in mind the three C's:

- Communication
- Collaboration
- Coordination

PART 2: DATA FLOW IN THE REAL WORLD

So, what can an organization do to make sure all incident-related data is flowing to the right place?

- Have effective strategies in place
- Communicate those strategies to the rest of the organization

However, this is not a challenge easily solved by off-the-shelf software. Incident response is a relatively new field; you can't go to Best Buy or Circuit City and buy a be-all, end-all security incident tracking solution.

Tools are emerging, but they are works in progress.

For effective incident tracking, an organization needs:

- A way to quickly identify and tag relevant information
- Searching capability
- Ability to collect information that may be adjunct to the incident report (such as log files or analysis results)
- Sorting capability
- Reminder capability
- Ability to share information in sanitized ways with external parties

Remember, incidents happen everywhere and can come from anywhere. So:

- Take an enterprise view.
- Recognize that response doesn't happen in isolation.
- Recognize that any type of incident management capability must support the organization's mission.

Conflicts may occur. You may have the technology to prevent or contain an incident; but it may cause more problems than it solves. Or, for example, a healthcare system may not be patchable without breaking FDA (U. S. Food and Drug Administration) certification.

In working through these conflicts, always keep in mind:

- What is the mission of the business?
- How does the incident management capability support that?

In a related vein, you must know:

- What are our mission-critical assets--systems, networks, applications, and data?

- And where are they?

People who are handling incidents may not have risk management skills and expertise, but they need to be working with people who do have those skills, to answer questions like:

- How critical is the affected asset and what is the potential impact of the incident?
- Can I patch it? Can I take it down? Can I do any type of mitigation?
- What type of problems will this cause my business?
- Who is the owner of this system? (the system owner may be the arbiter for what you can and cannot do)
- Who do I need to notify?

PART 3: THE FUTURE

How might incident management evolve over the next few years, and how can business leaders prepare for this?

Currently, there is more push in the community for standards and other ways to evaluate capabilities. For example:

- ITIL (Information Technology Infrastructure Library)
- ISO (International Organization for Standardisation)
- NIST (National Institute of Standards and Technology) best practices
- FIPS (Federal Information Processing Standards)
- Certification of teams and individuals

Incident management is still a fairly young field. So you need to determine:

- How does all this fit together with other continuity of operations functions across your organization?
- What are the triggers you may get from incident management personnel that are going to trigger people who are handling business continuity or disaster recovery?
- What type of plan and response do you want in place that is repeatable, with sufficient quality, and can minimize damage to your organization and ensure it meets its business mission?

Contingency plans are required. We often see organizations whose capabilities are very thin--maybe one person deep.

Leaders need to think in terms of avoiding single points of failure. One person is not enough and should not be handling every aspect of incident management. Food for thought:

- What if a key person leaves?
- What if something really goes wrong and this is more than that one person can handle?

Resources

Action List for Developing a Computer Security Incident Response Team

CERT's CSIRT Development Page
