INTERNET
SECURITY
SYSTEMS™

Computer Security Incident Response Planning

Preparing for the Inevitable

Introduction

Computers and computer networks have been part of the corporate landscape for decades. But it's only in the last five years that companies have started to connect these systems and networks to the outside world – suppliers, business partners, and the Internet. Unfortunately, in the hurry to get connected and jump on the e-business bandwagon, computer security is frequently given short shrift, placing corporate assets at risk.

The popular media is filled with accounts of recent Internet security problems, including the denial of service attacks against Yahoo!, eBay, Amazon, CNN, and others, several instances of data theft involving credit cards or personal information, and the "I Love You" virus/worm. Although the press devoted many column-inches and on-air minutes to these stories, they focused primarily on the exciting topic of "the chase" to catch the perpetrators, and generally ignored the more important topics of how frequently computer security incidents occur, how many companies' data is at significant risk, and the potentially devastating impact of computer security incidents on their victims.

The Computer Security Institute, among other industry analysis, reports that computer security incidents are widespread (*2000 CSI/FBI Computer Crime and Security Survey*, Computer Security Institute, March 2000). 90% of respondents detected computer security breaches in the previous 12 months, and 70% reported serious security breaches other than the most common ones (viruses, laptop theft, and employee "net abuse"), such as theft of proprietary information, financial fraud, system penetration by outsiders, denial of service attacks, and sabotage of data or networks. The survey also shows that attacks occur frequently, with 35% percent of those acknowledging attacks reporting between two and five incidents in the last year, and 19% reporting ten or more incidents. 71% of the survey's respondents detected instances of unauthorized access by insiders, demonstrating that even companies whose networks are not connected to the Internet are at risk.

The computer security industry offers a variety of solutions to this problem, from firewalls, authentication, and encryption to vulnerability scanning tools and intrusion detection systems. Consulting firms offer a broad range of security services, including security assessments, secure network infrastructure design and deployment, policy development, penetration testing, and so forth. But while all of these products and services have their place, they take time (often months, sometimes years) and money to procure and implement correctly. In the meantime, a company has to live with the security implementation it has – it may not be state-of-the-art, it may not be as strong as it should be, but the systems and networks that depend on it are critical to the company's business, and cannot simply be turned off while waiting for a stronger security solution to be designed and installed.

Given the certainty that attempts will be made to compromise system and network security, and the likelihood that these attempts will succeed, every company, large or small, must be prepared to respond effectively to security incidents when they occur. Even sophisticated, state-of-the-art security systems are not foolproof – thus, regardless of where a company is in the "security spectrum," an organized incident response capability is of the utmost importance.

Incident Response Planning

A Computer Security Incident Response Plan (CSIRP) provides guidance and documentation on computer security incident response handling and communication efforts. The CSIRP is activated whenever a computer security incident occurs, and guides the responses to all incidents whose severity is such that they could affect a company's ability to do business, or undermine its reputation.

The inevitability that (possibly successful) attempts will be made to compromise system and network security dictates that every company, from the largest multinationals to the smallest "dot com" startups, should have a formal CSIRP in place. CSIRP development should be the top security budget priority in any company – more important than security services, and more important than security products. When a security incident occurs, reactions and decisions must be made very quickly (often in a matter of minutes). The company has to be prepared to deal with these incidents as soon as they occur; waiting until a new product arrives or a consulting engagement is completed is not an option.

Establishing a Team

The first step in creating a formal CSIRP is the establishment of a Computer Security Incident Response Team (CSIRT).

The CSIRT Charter

The CSIRT Charter is a document that formally establishes the team, and documents its responsibility to respond to computer security incidents. The CSIRT Charter also delegates the authority to implement necessary actions and decisions during an incident, usually to the CSIRT leader or manager.

Sections of the CSIRT Charter document include:

> ***Mission*** – Describes the overall goals of the CSIRT; the things it is responsible for. This might include such tasks as responding to all incidents, minimizing their impact, and collecting data and evidence for prosecution.
>
> ***Scope*** – Defines the constituency of the CSIRT, i.e., who it serves. Some companies may have a single CSIRT for the entire company, while others may have multiple CSIRTs separated by business unit, geography, or other criteria. This section also describes the team's area of responsibility (e.g., all corporate networks, all networks in a division, all networks connected to the corporate network (such as those of business partners), or some combination thereof).
>
> ***Organizational Structure*** – Documents how the CSIRT is organized from a management perspective – how the members of the team are managed, and how the team reports to upper-level management.
>
> ***Information Flow*** – Describes how information flows before, during, and after an incident. First, this section describes how a potential security incident is reported to the CSIRT, and provides contact information for doing so. Second, it describes how the CSIRT communicates information about an incident to (a) upper-level management, (b) company employees, and (c) the public.
>
> ***Services Provided*** – Documents the specific services the CSIRT provides. This is based on the mission statement (above), and may include services such as incident response, policy development, compliance testing, and user education.

Roles and Responsibilities

A CSIRT usually consists of a manager, a management advisory board, some number of permanent team members, and a larger number of temporary members:

> ***CSIRT Manager/Leader*** – The CSIRT Manager (or Leader) is responsible for managing the overall response and recovery activities for all security incidents. He or she determines (usually with assistance from others) the severity of each incident, and decides which staff members will perform the actual response and recovery tasks. The CSIRT Manager usually has some degree of budget and decision authority to take necessary actions during an incident.
>
> ***Management Advisory Board*** – The management advisory board is made up of senior managers from the company's IT organizations and other internal business functions. IT organizations represented may include Network Services, Internet Operations, Mainframe Operations, Midrange Operations, Server Operations, Desktop Operations, and Help Desk. Other internal business functions represented may include Corporate Security, Legal, Human Resources, Media Relations, and Disaster Recovery. This group makes decisions and budget requests above the level delegated to the CSIRT Manager.
>
> ***Permanent Team Members*** – Permanent team members are those IT staff whose primary job responsibility is IT security. Usually, these people report to the CSIRT Manager. They provide the non-response services (such as user education and policy development), and help the CSIRT Manager in the initial response to incidents.
>
> ***Temporary Team Members*** – Temporary team members report to the IT organizations and other internal business functions represented on the management advisory board. They are the subject matter experts for the particular systems, applications, and business issues involved in the incident. Temporary team members are usually assigned to an incident by their managers (on the advisory board) at the request of the CSIRT Manager, and serve for the duration of the incident.

Within the CSIRP, it is important to document the specific roles and responsibilities of each of the above groups. Specifically, the following points need to be addressed:

- How much decision and budget authority is delegated to the CSIRT Manager? For example, can he or she authorize overtime? If so, how much? Can he or she authorize disconnecting the company from the Internet altogether? If so, under what conditions?
- What is each group responsible for? Every action to be taken should have an "owner" associated with it, to make sure it gets done. Where necessary, limits should be set and documented (e.g., a server can be taken down for less than an hour without authorization, but longer periods need the approval of someone higher up in the management chain).
- When major decisions need to be made (e.g., disconnect from the Internet, pursue the attacker vs. protect the systems, etc.), what are the criteria for those decisions? Who has the ultimate authority to make the decision?

The roles and responsibilities section of the CSIRP is perhaps the most challenging section to write. On the one hand, it has to be specific in answering the questions posed above, to avoid any ambiguities in interpretation. On the other hand, it has to be general, to avoid getting bogged down in too many details. The best CSIRPs approach this

conflict by being as general as possible, and only getting into specifics when absolutely necessary.

Incident Severity and Declaration

Many security incidents, such as isolated occurrences of computer viruses, are easily handled via well-established procedures (especially in larger companies), and do not justify calling out the entire CSIRT. The CSIRP must describe the criteria used to classify the severity of security incidents, and which severities will result in CSIRP activation.

Incident Severity

Incidents should usually be grouped into a few different severity levels, with broad sets of criteria for each level. For example:

> ***Severity 1*** – Small numbers of system probes or scans detected on internal systems; isolated instances of known computer viruses easily handled by anti-virus software.
>
> ***Severity 2*** – Small numbers of system probes or scans detected on external systems; intelligence received concerning threats to which systems may be vulnerable.
>
> ***Severity 3*** – Significant numbers of system probes or scans detected; penetration or denial of service attacks attempted with no impact on operations; widespread instances of known computer viruses easily handled by anti-virus software; isolated instances of a new computer virus not handled by anti-virus software.
>
> ***Severity 4*** – Penetration or denial of service attacks attempted with limited impact on operations; widespread instances of a new computer virus not handled by anti-virus software; some risk of negative financial or public relations impact.
>
> ***Severity 5*** – Successful penetration or denial of service attacks detected with significant impact on operations; significant risk of negative financial or public relations impact.

In this example, incidents of Severity 3, 4, and 5 would result in CSIRP activation, while incidents of Severity 1 and 2 would be handled without CSIRT involvement.

Incident Declaration

When an incident requiring CSIRP activation occurs, a formal incident is declared. The CSIRP should document how such a declaration is made and who is responsible for making it. Generally, incident declaration is a procedure by which the CSIRT Manager notifies upper-level management that an incident is taking place, and then assembles the other members of the CSIRT.

Response Procedures

Response procedures can be described at two levels of detail in the CSIRP. The first level of detail is a set of general guidelines that describes the principal phases of incident response, and what happens during each phase. Every CSIRP should include this level of detail. The second level of detail is a set of step-by-step response procedures, specific to individual incident types (e.g., procedure(s) for handling virus incidents, procedure(s) for handling hacker break-ins, etc.). These procedures will

generally be created over time, and can be added to the CSIRP in appendices as they are developed.

There are five principal phases of incident response, shown below. The general procedures to be followed in each phase should be described in the CSIRP.

Alert Phase
The alert phase is the process of learning about a (potential) security incident, and reporting it to the CSIRT. Alerts may arrive from a variety of sources including: firewalls and intrusion detection systems, anti-virus software, threats received via electronic mail, media reports about a new threat, etc.

The CSIRT is usually notified by providing a "hotline" telephone number, or a duty phone/pager that is reachable 24 hours a day, 7 days a week.

Triage Phase
The triage phase is the process of examining the information available about the incident to determine first if it is a "real" incident, and second, if it is, its severity. The CSIRT Manager usually does this, with assistance from the permanent team members.

If the incident's severity warrants, the CSIRT management advisory board will also be alerted in this phase. The board must do two important things in this phase:

- A decision to "pursue" or "protect" must be made. In other words, does the company want to attempt to catch the perpetrator(s) of the attack for later criminal or civil action, or does it simply want to stop the incident and restore normal operations? This decision must be made *before* response begins, because it influences how the response will happen.
- Resources (personnel and financial) must be allocated to the response and recovery teams at a level appropriate to the severity of the incident.

Response Phase
In the response phase, the CSIRT gathers evidence (audit trails, log files, contents of files, etc.). If the "pursue" option was chosen, this process must be performed in a forensically sound manner so that the evidence will later be admissible in court; the team may need specialized technical assistance and advice from a third party to do this successfully.

Once evidence has been gathered, it is analyzed to determine the cause of the incident, the vulnerability or vulnerabilities being exploited, how to eliminate these vulnerabilities and/or stop the incident, and so forth. An assessment is also made of how far the incident has spread, i.e., which systems are involved, and how badly have they been compromised.

Recovery Phase
The recovery phase begins once the response phase has been completed (there may at times be some overlap). In this phase, the CSIRT restores the systems affected by the incident to normal operation. This may require reloading data from backup tapes, or reinstalling systems from their original distribution media.

Once the affected systems have been restored, they are tested to make sure they are no longer vulnerable to the attack(s) that caused the incident. They are also tested to make sure they will function correctly when placed back into production.

Maintenance Phase

The maintenance phase is also called “lessons learned.” In this phase, the entire incident, as well as the response, are reviewed to determine which parts of the CSIRP plan worked correctly, and which parts need improvement. The areas in which improvement is needed are then corrected, and the CSIRP updated accordingly. Other areas that need to be changed (policies, system configurations, etc.) may also be identified during this phase.

The Advantages of Commercial Incident Response Services

In the last few years, Internet Security Systems and a handful of other companies have begun offering commercial incident response services. These services are usually subscription-based (although some companies will also provide ad-hoc assistance) and include both proactive and reactive components. The proactive components include such items as on-site consulting, policy review and/or development, vulnerability assessments, security advisories, etc. The reactive components usually involve telephone and/or on-site response to customers' security incidents by professionals experienced in computer security incident response disciplines.

When our children enter pre-school or kindergarten, one of the first things we teach them is how to dial 9-1-1 in an emergency. Because it is unlikely that a child can be taught how to properly respond to these emergencies (e.g., a heart attack), it is better to teach them how to quickly summon someone who can. However, even trained professionals (e.g., doctors) recognize that the people who respond to these calls are both better trained and better equipped to handle emergencies, and will therefore make use of 9-1-1 as well, if only to make sure that extra help is available if it is needed.

Commercial incident response services are built around the same thinking. On the one hand, there are numerous companies with little or no in-house IT security expertise. These companies need someone to respond to security incidents for them, because they cannot do it themselves. On the other hand, even large companies, with extensive IT security staffs, recognize the value of having experts on call that "live and breathe" computer security incident response and can offer advice and assistance.

Depth and Breadth of Experience

One of the most valuable components of commercial services is the depth of experience they bring to the table. Every member of the commercial service is experienced in computer security incident response, having responded to dozens, if not hundreds, of actual incidents. A single company's IT staff, on the other hand, has limited experience at best, because it only has an opportunity to respond to incidents affecting that company.

Commercial response teams also bring breadth of experience. Because they respond to incidents at multiple customers, they are exposed to a wider variety of systems, network configurations, and attack methods than a single company's team would be. In many cases, an incident that is new and unheard of to the customer's response team will already be familiar to the commercial response team.

Specialized Skills

Another valuable component of commercial response teams is the set of specialized skills they offer. This includes in-depth experience with a wide variety of operating systems and applications, but also less common skills such as forensics investigation and analysis.

Forensics

A few years ago, most computer security incidents were certainly annoying, and possibly embarrassing, but they caused little if any lasting damage. But as the trend toward e-business continues, this is changing. The CSI survey reports that 74% of respondents reported financial losses because of computer security breaches and misuse last year.

As the potential for actual loss increases, the response to incidents is changing. Where it used to be sufficient to simply make the problem "go away," companies are now becoming much more interested in pursuing legal action (criminal or civil) against the perpetrators.

To pursue such legal action however, evidence is needed, and this evidence must be admissible in a court of law. This means that the evidence must be collected and analyzed in a forensically sound manner, i.e., according to special rules of conduct on the part of the investigators. It is important to note that forensic investigation and analysis is *not* a technical problem, but a legal one. Specialized data-gathering equipment and data-analysis tools are needed to insure that evidence is not inadvertently altered or destroyed. The personnel performing the investigation and analysis must be specially trained to perform their jobs, and, if the case goes to trial, to testify about their actions in court.

Staff Costs

The last, and perhaps the most significant advantage of commercial incident response teams, is one of staff costs. Computer security personnel are in notoriously high demand, making them both expensive to acquire, and difficult to retain.

According to the SANS Institute, security administrators and consultants made average salaries of $63,598 and $79,395, respectively (*SANS Security Alert*, SANS Institute, January 2001). Add to this the expense of ongoing training, necessary to keep these employees' skills up-to-date, and the cost goes even higher. The Gartner Group estimates that a small, dedicated, two-person incident response team will cost $251,000 in first-year capital expenditures, $324,000 per year in salaries, benefits, and training, and $100,000 per year in external investigation and forensics services (Source: Gartner Group, October 2000). Justifying the funds to hire a dedicated staff of security personnel is difficult for many large companies, and frequently impossible for smaller ones.

Because the security job market is so volatile, retention is also a problem. Computer security incident response personnel would, on the whole, rather be responding to incidents. If a company does not suffer enough incidents to keep its staff occupied, those people are likely to go elsewhere, where things may be more "exciting."

Advantage

Commercial incident response services can help companies with all of these problems. They offer a pool of highly experienced staff, and make sure that they receive adequate training to keep their skills up to date. Because they can spread the costs over multiple customers, commercial services can offer specialized skills such as forensic investigation and analysis that would be unaffordable to a single company. And, again because they can spread the costs over multiple customers, they can offer their services to customers for little more than the cost of a hiring a single security expert in-house.

Summary

Every company needs to have a Computer Security Incident Response Plan in place, regardless of where the company is in the “security spectrum.” Security incidents won’t wait for new security software to be installed, or security consulting engagements to be completed. A company has to be prepared to defend what it has, and respond to security incidents as they occur.

Commercial security incident response services can help companies develop their CSIRPs, not only with consulting to build the plan itself, but also by providing response team personnel. A company can augment its own security staff, whatever its size and experience, with a commercial service to provide additional expertise and specialized skills. This partnership approach results in the best protection at the lowest cost.

About Internet Security Systems (ISS)

Internet Security Systems, Inc. (ISS) (Nasdaq: ISSX) is the leading global provider of security management solutions for the Internet. By combining best of breed products, security management services, aggressive research and development, and comprehensive educational and consulting services, ISS is the trusted security advisor for thousands of organizations around the world looking to protect their mission critical information and networks.