Dealing with External Computer Security Incidents

CERT® Coordination Center

Dealing with computer security incidents is extremely difficult. There are many ways that incidents can occur and many types of impact they can have on an organization. There are no complete solutions, and the partial solutions that exist are expensive and resource intensive. However, the alternative—not dealing with security incidents—is yet more expensive, and using weak methods for dealing with incidents may only compound the damage that incidents cause. What is required is a long-term commitment to develop the capability to deal with security incidents, not just make short-term fixes of selected problems.

A security incident is the act of violating an explicit or implied security policy at a single site or across multiple organizations. An external security incident is one caused by an individual or group not part of the organizations that are violated. This paper discusses some of the effort required to deal with external security incidents on an organization's hosts (computers) and network. We look at both responsive actions to incidents and proactive actions to mitigate the risk of such incidents. Because of inherent weaknesses in many of the current network protocols and vulnerabilities in widely used software, external security incidents are inevitable to any organization with a connection to a wide-area public network, even a narrow and limited connection.

A more lengthy discussion is found in the CERT Coordination Center (CERT/CC) document *Steps for Recovering from a UNIX or NT System Compromise* (http://www.cert.org/tech_tips/win-UNIX-system_compromise.html).

Prior to an incident

Organizations need to be prepared to deal with computer security incidents before they occur. This preparation includes ensuring that policy clearly designates who is to respond to the incidents, what authority these individuals have in responding to incidents, and what actions are permissible and forbidden. During an incident, events often move rapidly, and that is no time for discussions about who is responsible for response, or who is authorized to take response actions. This policy needs to be widely communicated to users and to system administrators.

Master copies of as-installed configurations of system and application software need to be created, kept up to date, and placed for rapid access by the authorized personnel. These master copies need to be carefully reviewed for malicious software; among the steps to take are scanning by virus checkers and using cryptographic checksum systems. The master copies should also include all critical configuration files and network operational data. In addition, backups of

organizational data must be taken frequently and validation procedures established to assure that these backups can be used to restore the data.

Organizations should establish external contacts to resources that may help them deal with security incidents. The vendors of critical operating system and application software often provide fixes to identified vulnerabilities in their software. If the organization or its parent department has established its own computer security incident response team, the contacts for that team must be identified as well. The FBI National Infrastructure Protection Center (NIPC) (http://www.nipc.gov, email: nipc@fbi.gov, contact via the local FBI field office) performs criminal investigation of security incidents.

During an incident, actions may need to be taken quickly. Thus, organizations should establish resources for effectively documenting what response actions were taken. This documentation can be critical for both technical and law-enforcement purposes. Technically, the documentation provides a basis for reviewing and improving both the computing infrastructure and the response procedures. For law enforcement, the documentation may provide a basis for assessing the impact of the incident and for evidence-collection actions. For more information on preparing for intrusions, see *Establish a policy and procedures that prepare your organization to detect signs of intrusion*. (http://www.cert.org/security-improvement/practices/p090.html)

During an incident

The first step in dealing with a security incident is regaining control of the organization's hosts and networks. The responders need to document what they know about the suspected incident, including its symptoms. Regaining control may involve physically isolating the affected hosts from the rest of the computing infrastructure and from the Internet. To assure a solid basis for examining the incident, the responders need to use low-level copying methods to make a complete copy of the disk and memory state of the affected hosts. They also should make a copy of all log files showing suspected intruder activity and make sure access to this copy is restricted to authorized personnel. At this point, the responders should have enough information to allow a close appraisal of the activity. They should begin by verifying that this activity indeed represents a security incident—many accidental conditions may appear to be intentional security violations. If in the technical judgment of the response team, a security incident cannot be confirmed, then the connectivity may be restored. Even if the incident is confirmed, ceasing service may be unacceptable, so one option is to replace a production host with a "hot spare" that has limited functionality, preserving the most critical mission functions but limiting the opportunities for compromise. In all cases, operation should be closely monitored.

Once control is regained and the incident is reasonably confirmed, the next step is to analyze the incident. This analysis involves a thorough review of the local operating system and configuration files for signs of intrusions. One resource that lists detailed steps for doing this review is *Detecting Signs of Intrusion*

(http://www.cert.org/security-improvement/modules/m01.html). Based on the review, the scope of response actions may need to be expanded or contracted.

Intruders frequently use compromised accounts or computers to launch attacks on other sites. If there is any evidence of compromise or intruder activity at other sites, it is important to contact these sites because may not be aware of the intruder activity. This contact can be done directly by the response staff or through a trustworthy intermediary such as the CERT/CC, which can contact the other sites while preserving the organization's confidentiality. (FedCIRC plays this role for government agencies.) The site needs to know what has been found, an explanation that this may be a sign of compromise or intruder activity at their site, and a suggestion that they may wish to take steps to determine if or how the compromise occurred and to prevent a recurrence. When contacting other sites or the intermediary, the responders should give as much detail as possible within the limits of the organization's security policy, potentially including date and time-stamps, timezone, and follow-up contact information. For more details, see the *CSIRT Handbook* (http://www.sei.cmu.edu/pub/documents/98.reports/pdf/98hb001.pdf). It is a good idea to "cc" the CERT/CC on your communication, in case the activity is part of a larger network security compromise that we are aware of. Information on finding site contacts is available from the CERT/CC (http://www.cert.org/tech_tips/finding_site_contacts.html). Additional information can also be found using the InterNIC whois database (http://www.internic.net/whois.html). It is normally *not* wise to contact an intruder directly—they may cause further damage to the organization's infrastructure in an attempt to conceal their activity.

After they analyze an incident, including any information gleaned via external contacts, the response team should be able to restore the affected hosts and network. Using the prepared master copies, they should install clean and patched versions of the operating system and applications software on the affected systems. If a machine is compromised, anything on that host could be modified; so the only way to be sure that a computer is free from intruder modifications is to reinstall all software and data from trusted and verified sources. In many cases, this involves using distribution media from the manufacturer. Following reinstallation, the computers should be configured to offer only the services that the system is intended to provide and no others. The responders should check that there are no weaknesses in the configuration files for those services and that those services are available only to the intended set of other systems. In general, the most conservative policy is to start by disabling all services and only enable services as they are needed. The responders should then apply the full set of security patches for each of the affected systems, as available from the vendor. As a further level of assurance, the responders should consult all external information on vulnerabilities, including information from the vendors and from CERT/CC advisories (http://www.cert.org/advisories). When restoring data from a backup, the responders should ensure that the restoration does not re-introduce a vulnerability that could be used by the intruder to regain access. Finally, the system administrators should change the passwords on all

accounts on the affected hosts, using passwords that are difficult to guess and that are not present in any dictionary.

To mitigate further security incidents, the organization should assess the security of its systems. There are a number of security guidelines, including the CERT/CC guidelines (http://www.cert.org/tech_tips/unix_security_checklist2.0.html and http://www.cert.org/tech_tips/win_configuration_guidelines.html). The value of the guidelines lies not in blocking all future incidents, but rather in removing commonly exploited vulnerabilities. *The Twenty Most Critical Internet Security Vulnerabilities* (http://www.sans.org/top20.htm) provides an abbreviated list of good things to do, some of which apply to current external security incidents, but intruders actively exploit a number of vulnerabilities beyond those listed in that document. Vigilance in monitoring hosts and installing vendor security patches is still required. To facilitate this vigilance, the organization should consider using some of the software security tools available both from vendors and from freeware archives on the Internet. The responders should install these tools before they connect the affected hosts back to the network, updating the master copies for future reinstallation if required. Hosts that have been compromised in the past tend to be at an increased risk for further intrusions, so system administrators need to ensure that all logging/auditing and accounting programs are enabled and that log files are diligently reviewed. Any installed intrusion detection systems should be updated to identify suspicious activity. The network administrators need to configure any available firewalls to restrict connectivity to the affected systems only to that required for their intended operation. Once this is done, the hosts and networks may be reconnected to the organizational infrastructure and, if desired, to the Internet.

Following an incident

Using their records of the actions performed during the incident, the response team members and their management should document lessons learned from the incident. This practice can result in continued improvement of the organization's security stance. One document that can aid in the improvement of the organization's security policy is the *Site Security Handbook* (ftp://ftp.isi.edu/in-notes/rfc2196.txt). Management should calculate the costs of the incident as a basis for prioritizing improvement in security. Following an incident, it is particularly urgent to keep the organization's personnel informed as to the changes in the security policy and how these changes may affect them.

Sources of further information

http://www.cert.org

- Descriptions and statistics of current Internet intrusion activity
- Advisories documenting a variety of significant vulnerabilities
- Reports on security-related topics
- Guidelines for configuring systems and for detecting and reporting incidents
- Security improvement modules and technical tips
- Training course schedule

http://www.fedcirc.gov

- Descriptions and statistics of current incidents affecting the Federal Government
- Links to a variety of information related to security in the Federal Government
- Descriptions of tools to support security in Government systems
- Event calendar
- Links to other security sites

http://www.nipc.gov

- Advisories of significant incident activity
- NIPC organizational, mission and contact information
- Links to other security sites and news
- Links to information on ethical use of computers

http://www.sans.org

- Events
- Publications
- Online reports
- Mailing lists