Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Corporate Incident Handling Guidelines

Incidents are an unfortunate fact of life in any systems environment. They can be extremely visible and disruptive (e.g.: widespread virus outbreaks) or entirely unnoticed but extremely damaging (e.g.: loss of confidential growth plans). There is a vast amount of information available to help you deal with most types, but if you have done no preparation you will struggle to find it when you need it at short notice. Incidents are also likely to occur at the least convenient time when the right people are not available. ...

Copyright SANS Institute
Author Retains Full Rights

AD

GSEC Version 1.2f
Administrivia Version 2.0

Corporate Incident Handling Guidelines

David Theunissen
14 November 2001

Incidents are an unfortunate fact of life in any systems environment. They can be extremely visible and disruptive (eg: widespread virus outbreaks) or entirely unnoticed but extremely damaging (eg: loss of confidential growth plans). There is a vast amount of information available to help you deal with most types, but if you have done no preparation you will struggle to find it when you need it at short notice. Incidents are also likely to occur at the least convenient time when the right people are not available. If you are a large multinational corporation without a large security function, this paper will help you approach some of the common problems in preparing incident handling procedures.

Sponsorship

As with most large corporations, it can take some time to bring ideas to fruition. The process I will describe will take many months to complete so it requires strong commitment. Naturally the time it takes will depend on the size and complexity of your organisation. I will touch on some of the organisational issues, but the BSI guidelines on Incident Handling [1] provides additional insight into some of these issues.

You will need high level agreement to adopt incident handling procedures, someone to investigate the issues and thorough review processes to involve those who are affected. You then time to incorporate them into work practices around the organisation. Each of these will have its challenges and can therefore take some time.

The purpose of having incident handling procedures is to know what to do when an incident occurs. This means anticipating scenarios before they happen, and making many decisions about them in advance. Decisions often require consultation and senior management agreement, so you will need these people on your side early in this process. For instance, simply deciding who to tell when an incident occurs can be hard to decide. Some things are confidential and should be kept at the strictly 'need to know' principle (eg: espionage). Some require your best people to respond quickly and this gets into issues like after hours support and mixed project/support roles. You may need external support and this costs money and takes time and effort to select partners. You will end up with a very 'woolly' procedure if you can't get management to agree formally to a robust structure and to make some important decisions up front.

The process of thinking through the typical incidents is an excellent risk analysis of your business as it makes you think through many of your vulnerabilities. For instance identifying that you need to have tools to test servers after eradicating malicious code should remind you of the fact that you should have these tools already! If you don't already have them it presents a great opportunity to secure commitment to select them. Eric Cole's web site has a good list [2] and the Sam Spade

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

site [3] has another approach. Your project to develop incident procedures will therefore start generating various improvement projects which can only be adopted with senior support.

Project Resource

There are vast amounts of excellent materials to help you handle incidents. The hard part, however, can be finding these at short notice which is why you need to develop procedures in advance of incidents occurring. The next challenge is to sift through all this material and select the parts which will be most helpful to your organisation. This requires a focussed project and someone who is given the time to do the work. Planning and preparation are key to many initiatives, and the effort you put into preparing your first draft procedure is key to engaging the people who have to use them later.

I started with the SANS Step by Step guide to Incident Handling which can be purchased from their online bookstore [4]. Their generic steps of preparing, identifying, containing, eradicating, recovering and following up are excellent. They can be applied in any level of detail to almost any problem. Just having this logical structure is an important first step. I start my incident handling procedures with a one page summary to be used as a quick reference, and these six phases appear prominently.

It's worth pointing out that the SANS document is about 36 pages long. It is crammed full of nuggets of information but you probably won't be able to include everything in your organisation's procedures. However, each point invokes thought, and thinking requires focussed attention and adequate time. You will have gathered information from other sources and you will need to extract and merge all the parts that are most relevant to your organisation.

Definition

Any document on any subject needs to have a scope. My first thoughts on incidents were that they can be any real or perceived occurrence which is out of the ordinary. However, it became clear to me that people struggle with definitions which are too open-ended or too complex. Hoaxes and threatened occurrences are generally regarded as valid 'incidents', so we ended up including this principle from the SANS document [4] into the shorter CERT/CC definition [5]. This is what we ended up with:

"The act of violating or threatening to violate an explicit or implied security policy"

As background to this document we had recently issued a high level user orientated security policy but many of our more detailed policies were still out of date. We therefore wanted some timeless and common sense/best practice elements while still retaining a punchy one-liner. We felt this definition provided all these features.

Generic Steps

There are some basic precautions or steps to take for each of the six phases described in the SANS guidelines [4]. These are covered well in that document but pose some

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

challenges when they come to actual implementation. Some of these are highlighted in the following sections.

We have a well-developed Help Desk support organisation and this is our standard mechanism for reporting problems or logging queries. Since many incidents will start off being a mere comment or inquiry about something appearing to be out of the ordinary, this is the appropriate reporting mechanism for us. However, you need to define when something should be handled differently or treated as an Incident. After-hours processes are particularly important as there will be fewer people to help make the right decisions. We cover the basic reporting process in the generic steps, and then described where deviations were required in the incident specific section.

Evidence

The collection of evidence is a complex and time-consuming process. There are a number of excellent introductions to the subject in the SANS Reading Room and I have highlighted one in my links below [6]. While thorough evidence collection has to be important, so is speed when it comes to containing incidents. Finding the balance between the two is challenging and we found it difficult to define.

Backups are an extremely important mechanism for gathering evidence but standard programs may have been modified in a rootkit attack and the normal programs won't create a mirror image of a disk. Any backup is better than no backup, but its usefulness will sometimes be dependant on the process followed and tools or media used. For instance, merely powering a computer on or off or connecting or disconnecting devices will change settings and delete items. If the sequence of events is wrong or remote attackers are alerted prematurely, your backup may not capture everything of importance whether needed in a court of law or just for internal diagnosis.

The cautious approach which will maximise the collection of evidence is to call in forensic experts and plan the approach very carefully. However, this will usually mean that you cannot be very responsive. It also means you probably stay vulnerable for longer. So consideration needs to be built into your process to solving this dilemma. It is difficult to be specific when you are trying to cover every permutation. We approached this issue by creating some decision criteria, examples and consultation guidelines. For instance, inappropriate use of computing resources by employees may lead to disciplinary action and even termination of employment. It will therefore be important to get a view from Human Resources and Legal as to the likely course of action and to balance this against the need for stealth, speed or thoroughness. For instance, should an employee sue you for what they consider to be unfair dismissal, you had better be able to prove guilt conclusively. Should a more forensic approach be called for, an external expert will have to be selected or you will probably need to recruit or train internal staff members. Regardless of the approach, a thorough awareness of the issues is important to prevent evidence from being becoming unusable.

Contain or Retain

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Another challenge is how radical or extensive to be in your containment efforts. A virus outbreak on one server can easily spread to others, but disconnecting many servers or a complete subnet prematurely causes significant business disruption. Once again we used the incident-specific guidelines to describe various scenarios and exposures. We have tried to give support staff the authority to act with speed when needed to contain destructive attacks and to be more consultative in other circumstances. This requires an element of risk taking as you end up giving written authority to act in defined circumstances which most managers would prefer were left open for them to exercise their discretion. Your approach will depend on the personalities involved and appetite for responsiveness and empowerment. Whatever you decide, it will give staff comfort that you have told them how to behave when confronted with some difficult scenarios.

You also need to decide the relative importance of detection versus containment. If you want to discover the most about an attack you may need to retain connections. Containment would normally call for quick severing of services. Honeypots and treasures are described quite well in an article by Michael Clark on the SecurityFocus web site [7]. Our view is that we are unlikely to establish such mechanisms due to the effort involved and risk of increased determination by the attacker. However, they may suit some organisations or scenarios. What this highlights is the need for you to formulate a position statement to help people make speedy decisions when confronted with difficult situations.

Level of Detail

As may have emerged from the above discussion, I decided that I wanted fairly detailed guidelines on how to handle incidents. I wanted these not only to help people handle specific incidents, but also to educate people about security and incident handling. I wanted high level management to understand some of the difficulties involved and the need for ongoing investment. I wanted the more hands-on people to think about the complexities before they rushed in to solving problems. I also wanted to start nurturing improved security awareness and practices in day to day activities to prevent incidents from happening in the first place.

The SANS guideline [4] provides a few pointers to incident-specific issues but I devoted almost half of my document to itemised checks or procedures. The CERT/CC Vulnerability Notes Database [8] will take you to the next level of detail. Even this database (quite correctly) often falls short of telling you how to use the tools it recommends. So this in turn will probably lead you to the realisation that more of your staff will need training or that you need outside experts to help you.

I chose the following high level categories for incident specific guidelines. I started with about a page on each and will expand on them and add more categories as our experience grows. For instance I have grouped web site, network and email denial of service together when they could each have their own specific guidelines. My view was that if I tried to outline everything in the first version, the task would be too great and the benefits of having a document in circulation and in use would be delayed.

- Denial of Service (including Email Bombing or Spamming)
- Email Spoofing

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

- Espionage (including Blackmail)
- Fraud, Theft and other Physical Incidents
- Inappropriate Use
- Malicious code (including Viruses)
- Probes and Network Mapping (including War Dialling)
- Unauthorised Access (including Network Intrusion, Sabotage and Web site defacement)
- Unlicenced/Pirate software
- Warnings and Hoaxes

You need to retain an element of dynamic updating if you do start exposing some of the detail involved in each of the above categories. New issues keep emerging and some excellent web sites are available to research specific issues. Hoaxbusters [9] will help eliminate the false alarms. The ICAT site [10] is particularly good with real vulnerabilities as it allows you to search by products or vendor. This is based on the Common Vulnerabilities and Exposures (CVE [11]) naming convention which standardises exposures making them easier to cross-reference. It includes a severity indication which is really helpful in assessing the urgency needed and provides information or links to sites which tells you how to handle the issue. Links such as these need to be incorporated into your procedures document so that your target audience can find them easily.

Deployment

You will need to ensure that all affected departments review and sign-off your procedure document. This is likely to include IT, Human Resources, Legal, Public Relations, Risk Management, Safety and Security if you have these functions.

You may then also have quality processes into which your document and revised processes will need to be incorporated. You will have to arrange for local and global contacts lists to be included. Enquire about business Crisis Communications plans as a major security incident could invoke these. The procedures may trigger some unease in some quarters if you include too much detail so look for these signs. Try to make sure that local managers acquire toolkits and include training needs in personnel and annual plans.

We found that our internal problem prioritisation / severity classifications had to be updated as incidents had not been anticipated in the way in which they were described. For instance, the compromise of one text document would typically not receive the highest priority, but if it was a year end financial report it probably should.

If you are a global organisation with varying degrees of control over subsidiaries, then you will need to ensure that the document is distributed to every region. If you outsource significant functions you will need to ensure that your procedures reach these providers.

You will need to comply with local legislative requirements. For instance the UK Data Protection agency [12] is a source of advice on handling confidential personal data which may be relevant during investigations. The site contains links to European Union guidelines on dealing with other countries. These are regarded by many as the

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

most restrictive in the world although every country will have its own specific requirements which will need to be considered.

You are encouraged to report incidents to your local computer incident response team (CIRT). The CERT/CC web site [13] describes the process and has some international links.

Conclusions

Hopefully this paper has given readers an insight to the process of developing incident handling procedures for a global corporate. I have tried to highlight some of the challenges and a few policy decisions which may be needed. It is considerable work to do properly, but is worth doing if it helps your entire organisation address incidents in a timely and controlled manner.

References

1. BSI (Bundesamt für Sicherheit in der Informationstechnik). "IT Baseline Protection Model" - S 6.58 Establishment of a management system for handling security incidents
   http://www.bsi.de/gshb/english/s/s6058.htm

2. Cole, Eric. "Security Haven / Hackers Beware"
   http://www.securityhaven.com/tools.html

3. Sam Spade.
   http://www.samspade.org/

4. SANS Institute Bookstore. "G4.1 - Computer Security Incident Handling: Step-by-Step"
   http://www.sansstore.org/

5. CERT Coordination Center. "Incident Reporting Guidelines"
   http://www.cert.org/tech_tips/incident_reporting.html

6. Lunn, Dorothy A. "Computer Forensics – An Overview"
   http://www.sans.org/infosecFAQ/incident/forensics.htm

7. Clark, Michael. "Virtual Honeynets"
   http://www.securityfocus.com/cgi-bin/infocus.pl?id=1506

8. CERT Coordination Center. "Vulnerabilities Notes Database"
   http://www.cert.org/nav/index_red.html

9. Hoaxbusters.
   http://hoaxbusters.ciac.org/

10. ICAT. "CVE Vulnerability Search Engine"
    http://icat.nist.gov/icat.cfm

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

11. CVE. "Common Vulnerabilities and Exposures"
http://www.cve.mitre.org/

12. Data Protection Commissioner. "Principles of Data Protection
http://www.dataprotection.gov.uk/principl.htm

13. CERT Coordination Center. "Incident Reporting Guidelines"
http://www.cert.org/tech_tips/incident_reporting.html#III

© SANS Institute 2001, Author retains full rights

Last Updated: February 9th, 2016

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Northern Virginia - McLean 2016	**McLean, VAUS**	**Feb 15, 2016 - Feb 20, 2016**	**Live Event**
SANS Munich Winter 2016	**Munich, DE**	**Feb 15, 2016 - Feb 20, 2016**	**Live Event**
ICS Security Summit & Training - Orlando	**Orlando, FLUS**	**Feb 16, 2016 - Feb 23, 2016**	**Live Event**
SANS Secure India 2016	**Bangalore, IN**	**Feb 22, 2016 - Mar 05, 2016**	**Live Event**
SANS Southern California - Anaheim 2016	**Anaheim, CAUS**	**Feb 22, 2016 - Feb 27, 2016**	**Live Event**
RSA Conference 2016	**San Francisco, CAUS**	**Feb 28, 2016 - Feb 29, 2016**	**Live Event**
SANS Philadelphia 2016	**Philadelphia, PAUS**	**Feb 29, 2016 - Mar 05, 2016**	**Live Event**
SANS London Spring 2016	**London, GB**	**Feb 29, 2016 - Mar 05, 2016**	**Live Event**
SANS Abu Dhabi 2016	**Abu Dhabi, AE**	**Mar 05, 2016 - Mar 10, 2016**	**Live Event**
SANS 2016	**Orlando, FLUS**	**Mar 12, 2016 - Mar 21, 2016**	**Live Event**
ICS410 Dubai 2016	**Dubai, AE**	**Mar 13, 2016 - Mar 17, 2016**	**Live Event**
SANS Secure Singapore 2016	**Singapore, SG**	**Mar 28, 2016 - Apr 09, 2016**	**Live Event**
SANS Atlanta 2016	**Atlanta, GAUS**	**Apr 04, 2016 - Apr 09, 2016**	**Live Event**
SANS Northern Virginia - Reston 2016	**Reston, VAUS**	**Apr 04, 2016 - Apr 09, 2016**	**Live Event**
SANS Secure Europe 2016	**Amsterdam, NL**	**Apr 04, 2016 - Apr 16, 2016**	**Live Event**
Threat Hunting and Incident Response Summit	**New Orleans, LAUS**	**Apr 12, 2016 - Apr 19, 2016**	**Live Event**
SANS Pen Test Austin	**Austin, TXUS**	**Apr 18, 2016 - Apr 23, 2016**	**Live Event**
SANS Secure Canberra 2016	**Canberra, AU**	**Apr 18, 2016 - Apr 23, 2016**	**Live Event**
ICS Amsterdam 2016	**Amsterdam, NL**	**Apr 18, 2016 - Apr 23, 2016**	**Live Event**
SANS Copenhagen 2016	**Copenhagen, DK**	**Apr 25, 2016 - Apr 30, 2016**	**Live Event**
SANS Security West 2016	**San Diego, CAUS**	**Apr 29, 2016 - May 06, 2016**	**Live Event**
SANS Secure Japan 2016	**OnlineJP**	**Feb 15, 2016 - Feb 20, 2016**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**