Global Information Assurance Certification Paper

SANS Security Essentials
GSEC Practical Assignment
Version 1.2d

Prosecution, A Subset of Incident Response Procedures
Gary T. Pasikowski
May 2001

Introduction

As the Internet has become a global marketplace, the World Wide Web has also grown exponentially; moreover, instead of slowing, its growth is only increasing. The web growth is mirrored in corporate growth as each company develops more complex information systems. The systems themselves are growing in complexity and, in turn, growing in the extent to which they are valued by the corporation and depended upon for its very existence.

When a company reaches the point where its very survival depends on the functionality of its system, the threat of outside interference (i.e., a hacker) can also represent the very real possibility of plunging stock prices and/or bankruptcy. Where this threat may have been an exaggeration a few months ago, enough corporate information is vulnerable to security breaches that large sections of the economy could be compromised by virtue of a hacked system.

Given that security breaches are a fact of life for businesses, the next question becomes one of response and the formation of sound security policies. While many guidelines and "how to" papers that will provide administrators with step-by-step instructions on dealing with a "typical" attack, the truth of the matter is that very few aspects of security can be called typical. The response to the attack should vary with the situation, the system in question and the attack approach that is used.

In order to prepare for such a series of variables, an administrator needs to take a top-down view of their entire network. Each piece of the system must be examined sequentially and, for each component, the question of "what if?" must be asked. Examples of the "what if" scenario should include the possibility of losing data resources, having the system usurped to facilitate other attacks, and even the destruction of the system itself.

As the administrator considers this series of questions for each system component, a thorough set of incidence response procedures can be developed. Thus, the administrator will not only be better prepared for the attack, but will also be prepared in the event that the company is able to prosecute the attacker.

The incidence response procedures form the crux of a sound and legally defensible security policy.

Background

In order to properly frame the context of the remainder of this paper, the following material has been prepared to give the reader information relating to incident response procedures and the Incident Response Team. Because of the sensitive and legally incriminating nature of an incident, the team approach (sanctioned by a corporate executive), is the best means for determining if, when and how a lawyer should be retained.

The Incident Response Team is responsible for responding to major security incidents that impact the health and welfare of the company and its customers. The team, for a moderately sized company should consist of someone from the senior management team, the Vice President of Information Services or CIO, the Corporate Security Officer, and the liaison for Public Affairs. The purpose of incident response procedures is to provide a set of general procedures for responding to security-related incidents. (It is important to note, however, that these procedures must be dynamic; as a business becomes more dependent upon their systems, their incident response procedures must reflect the ensuing changes.) The following table outlines the responsibilities and pertinent parties for a set of Incident Response Procedures.

Responsibility	Responsible Parties	Comments
Overall responsibility for the procedures	Corporate Security Officer	
Reporting security incidents	All associates, contractors and agents	Encourage incident reporting by contractors and agents through a security awareness program
Incident response management	Incident Response Team CSO or ISA (Based on the severity of the incident)	The Incident Response Team consists of a Senior Management Team Member, the Corporate Security Officer (CSO), the Vice President of Information Services, and the liaison for Public Affairs. Team members may delegate authority.
Carrying out required actions	Department heads of organizations identified in the procedures	Generally, the departments are Information Services, Human Resources and Public Affairs
Training and awareness of incident response procedures	Corporate Security Officer	Department heads are responsible for insuring their departments are capable of required response
Reviewing, updating and distributing incident response procedures	Corporate Security Officer	Department heads are responsible for distributing changes within their departments

Justification for a Lawyer

Lawyers who specialize in criminal computer activity are becoming more of a necessity. Before a company can justify the need for a lawyer, however, they must place a value on each resource that may be compromised. The Incident Response Team should outline all the resources and their approximate value to the company to allow corporate executives to justify the expenses of retaining a lawyer.

While the ethics of the situation may call for prosecution in every case, a business case should always be based on a cost factor. For example, it would not be in the best interest of a company to hire a lawyer if the cost of prosecution outweighs the cost of simply fixing the means by which the attack was manifested. In each attack scenario, the company has two choices: retain a lawyer in advance or wait until an event occurs that requires a lawyer. Depending on the risk that a company is willing to take, a lawyer may only be needed initially to review procedures and establish that pertinent points are included from the standpoint of legal precedence.

Importance of a Lawyer

Some companies may question the need for a lawyer to get involved in their computer related incidents. Research has shown, however, that in the case of a company that identifies a compromised system, an attorney can have a great impact in the investigation and gathering of the evidence. Evidence, or lack thereof, can make a significant difference in the case. For example, according to former America Online assistant general counsel Christopher G. Bubb, "It is a specialty, like contracts law, or deal law." Bubb, who participated in the 1999 Melissa virus investigation also stated, "That case hinged on information gathered by AOL's security department, with the careful guidance of the company's legal team." (http://www.securityfocus.com/news/185)

In a different case situation, the impact of a lawyer essentially means the difference in maintaining a corporate image or suffering a deluge of lawsuits from injured parties. Because many companies are establishing an e-commerce presence in addition to their 'brick and mortar' business, they are also becoming involved with database servers that store sensitive customer information — including credit card numbers. The value of the system in the event of a virus that damages the operating system is relatively low, because the administrator can perform a restore of the system usually very quickly. In the event of a compromise by an attacker who steals all the information, the value of the system is very high. A company may be faced with future lawsuits, and diminished reputation and trust in the eyes of their customers.

The Evidence

Many administrators never realize that the system at hand and the data on it could be evidence; most tend to concentrate on recovery. A typical example is found when inappropriate material is discovered on corporate PCs. When an administrator

investigates such a case, the pursuit is usually to "bust" the perpetrator. By faking a network problem in the building and pretending to conduct maintenance on the PCs, the culprit can usually be discovered. This method of flushing out a suspect is seldom successful, however, as most people who perform illegal actions are very suspicious of personnel in their area. As soon as they would leave the computer in question the evidence can mysteriously disappear. The implementation of third party monitoring software can be a great asset in these situations.

This case leads to an important factor that must be considered prior to contacting a lawyer: the evidence of an attack is almost as important as the system itself. A company's rule of thumb should be: *Approach every attack, and gather evidence as though it may eventually be used in court to prosecute an attacker*. The evidence gathered from an attack, although it may have been on a system deemed 'non-critical', may be very important — especially if the same attacker were to attack a critical system and a criminal case were involved.

Evidence is crucial for any company that chooses to retain a lawyer for computer criminal activity. The major factor in computer crime is that it is usually the company itself (versus a professional investigator) that gathers the evidence. This makes it imperative for company personnel to be properly trained and prepared to know in advance what type of data they will be gathering. If a company does not feel comfortable gathering evidence on a case, there are contract experts who can be employed.

According to a vnunet.com news article, administrators destroy evidence before it has a chance of being collected.

> The immediate resolution of the problem by internal system administrators and IT personnel can compromise the integrity of the data and corrupt the evidence of the breach. The likelihood of the company then being in a position to recover assets or pursue legal action will be low.
> (http://www.vnunet.com/News/1120289)

Since the evidence may be the most valuable aspect after an attack, there are things a company can do prior to hiring a lawyer. If, for example, a company's database server (containing sensitive customer information) was compromised, then it may not be clear whether the attacker has captured any of the information on the server. From previously outlined Incident Response Procedures, however, this server would have been deemed valuable enough to pursue legal action.

This is also an example where a company may want to bring in an expert to gather the evidence, as many companies may not have the expertise to properly handle the evidence. According to a recent survey, " U.S. companies spent $118 million on computer forensics and other incident response services in 2000, and are expected to more than double that to $277 million by 2004." (http://www.sfgate.com/cgi-bin/article.cgi?file=/chronicle/archive/2001/02/26/BU69784.DTL&_ref=14450787)

Even though cost is still the determining factor, the fact remains that the server contains very valuable information. The company cannot afford to be wrong.

It may not be clear, until after the evidence is analyzed, if a company should pursue prosecution. A company should include the following procedures relating to evidence in their Incident Response Procedures for just that reason. After the evidence is fully gathered will the company, the corporate executive will then be in a position to decide about hiring a lawyer.

1. Perform a full backup of the server.

   Do this before the server is removed from the network. Trojans are getting more sophisticated every day and there may be one located on the system which knows it has been removed from the network. This tells the Trojan that it has been discovered. As a precaution then, it destroys all data on the drives, and any evidence along with it. If it is possible, remove and retain the original hard drives.

2. Keep a log book

   Logging of information is critical in situations that may eventually involve federal authorities and the possibility of a criminal trial. The implications from each security incident are not always known at the beginning of, or even during, the course of an incident. Therefore, a written log should be kept for all security incidents that are under investigation. The information should be logged in a location that cannot be altered by others. Manually written logs are preferable since on-line logs can be altered or deleted.

   The types of information that should be logged are:

   -Dates and times of incident-related phone calls.
   -Dates and times when incident-related events were discovered or occurred.
   -Amount of time spent working on incident-related tasks.
   -People you have contacted or have contacted you.
   -Names of systems, programs or networks that have been affected.

3. Control the release of information

   Control of information during the course of a security incident or investigation of a possible incident is very important. Providing incorrect information to the wrong people can have undesirable side effects, especially if the news media is involved. An improper release of information could alert the perpetrator, and cause customers to lose confidence. Public Affairs or the CEO must authorize all releases of information. All requests for press releases must be forwarded to Public Affairs. Also, incident specific information, such as accounts involved, programs or system names, are not to be provided to any callers claiming to be a

security officer, law enforcement official or an unknown internal caller. All suspicious requests for information should be forwarded to the Chief Security Officer or Information Services Analyst.

Conclusion

Unfortunately, there are no definite rules for dealing with the legal issues surrounding computer crime. A company must be prepared to prosecute whenever an attack occurs, but this information actually has to be outlined in their Incident Response Procedures *before* the attack occurs. If and when the situation arises then, the company will be properly prepared to pursue legal action and to decide if retaining a lawyer is the right option for the particular situation at hand.

References:

1. Poulsen, Kevin. "Hacked? Call a Lawyer." 4 April 2001. URL: http://www.securityfocus.com/news/185
2. Author Unknown. "Computer Crime Investigation & Computer Forensics." Information Systems Security. Summer 97, Volume 6, Issue 2: p56, 25p URL: http://telecom.canisius.edu/cf/computer_crime_investigation.htm
3. O'Brien, Kevin A. "The fight against cyber-crime." 1 December 2000. URL: http://www.mail-archive.com/cybercrime-alerts@topica.com/msg00156.html
4. Gaudin, Sharon. "Legal system gears up for computer crime cases." Network World Fusion. 27 June 2000. URL: http://www.cnn.com/2000/TECH/computing/06/27/computer.law.idg
5. Hayward, Douglas. "Who's Afraid Of The Big, Bad Hacker?" URL: http://www.techweb.com/wire/news/jul/0707hacker.html
6. McCue, Andy. "Users destroy vital e-fraud evidence." URL: http://www.vnunet.com/News/1120289
7. Goslar, Martin, Ph.D. "You've been hacked: Should you tell the world?" URL: http://www.zdnet.com/enterprise/stories/main/0,10228,2652725,00.html
8. Kirby, Carrie. "Cyber Sleuths, Computer forensics boom as importance of electronic evidence grows." URL: http://www.sfgate.com/cgi-bin/article.cgi?file=/chronicle/archive/2001/02/26/BU69784.DTL&_ref=14450787
9. Winegarden, Jerry. "What To Do if Hacked or Attacked." URL: http://www-jerry.oit.duke.edu/linux/bluedevil/HOWTO/what_to_do_if_hacked.html

Last Updated: July 22nd, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor