

Moment's Notice: The Immediate Steps of Incident Handling

Ben Malisow 2000-07-07

Introduction

The response to systems security incidents is as, if not more, important as detection. What actions you perform subsequent to identifying an incident will not only affect your organization's operations, but may impact future such procedures, your security posture, and the outcome of the situation.

This article covers the topic of response, including matters of scale, operational constraints, appropriate countermeasures, legal concerns, and hints for proper implementation. While not technical in nature, this study of response procedures might give you some insight on how to handle the more ambiguous elements of systems security: human factors, policy, and time.

Size does Matter

The scale of your response is obviously dictated by the nature of your organization. While a mom-and-pop retail store with an online merchandising site that comprises 5% of total annual revenues can disconnect their network at a moment's notice, and leave it off indefinitely, an organization rooted in e-commerce might be considerably harmed by responding in the same manner, depending on the duration of the response.

The focus of the organization is paramount to the means and extent of dealing with security incidents. The manner in which you eventually resolve the incident will determine the means with which to conduct the initial response. This may sound like putting the cart before the horse, but is, in fact, relevant.

Public sector organizations have ready recourse to some law enforcement branches that otherwise may not be employable for handling commerce-oriented incidents. For instance, government agencies can consult the intelligence and legal branches of the particular arm of bureaucracy "owning" them: for those under the auspices of the Department of Defense, there are almost limitless groups you can contact to deal with intruders, such as the Defense Investigative Service (DIS), the law enforcement component of the given branch of the military your organization falls under (Air Force Office of Special Investigations, etc.), Naval Counterintelligence Service, the FBI, and so forth; for non-military government agencies, the

Department of Justice and the Attorney General's office can assist; for non-federal government organizations, the state attorney general or local district attorney can handle the matter.

The benefit of eliciting response from those entities is the vast resources you can bring to bear to defend the integrity of your system after an incident has occurred. Prosecution, an otherwise expensive and involved process, is readily available to those who protect government systems.

If, on the other hand, you are working in the private sector, law enforcement agencies may be more or less inclined to assist, depending on the size and breadth of your company; if Yahoo! asks the federal government to become involved in an incident, it is much more likely the appropriate law enforcement arm will respond than if Bill's Bargain Basement Porn Site (with 100 users) makes such a request. While this may seem unfair or unjust, it is simply pragmatism: even the government has limited resources to conduct legal endeavors, and must protect the greatest number of people with those resources.

Realistically, contingency planning is necessary to determine whether or not prosecution is a likely means of recuperating value for your company. How you react in those first few minutes of an incident can make legal efforts untenable or relatively painless.

Another reason the size of your organization will in some manner dictate your level and means of response is the burden incident responses place on available personnel. If you are protecting a website by making one network person take on additional duties and calling that your "security team," you are in no position to maintain both operational capability and dramatic, continual incident response. A permanent, dedicated security team, tasked solely with information protection duties, can substitute system-hardening efforts for incident response activities at any time, all the time.

Furthermore, outsourcing systems or security functions may leave your organization in an even less-advantageous position to conduct timely, effective incident response procedures. The likelihood of your network being attacked at the same time as your contractor's other customers is quite good, making the likelihood of receiving priority assistance quite bad.

Aside from personnel issues, your organization has to decide what amount of systems is appropriate for incident defense, response, and recovery. Full redundancy of all systems? One backup "backbone" network to conduct emergency activities in the event your daily systems are compromised? Partial elements of both types?

Once again, you're faced with the main onus of security: planning. Your response will never be the same as any other given organization's response- it will be dictated by your needs and resources. Risk assessment is the operative element of any such planning: what are you trying to accomplish by your response? Operational recovery? Maintenance of consumer faith, branding, and market share? Protection of information? What are your plausible levels and means of response? Can you realistically involve law enforcement or legal countermeasures in a cost-effective manner?

Knowing what you can do, in large part, will dictate what you will do.

Attention to Detail

Whatever method of response you choose to employ, documenting the steps of your response is crucial not only to the immediate effort, but how future such security matters will be handled. One of the most frustrating and mundane chores is trying to reconstruct the activities of a response has occurred; learning to be aware and record events as they transpire will streamline your analysis of incident responses, and attenuate the problems associated with future such operations.

Have the proper implements and systems in place to conduct even simple record-keeping practices; if you plan to use your desktop workstation to document your response activities, you will be hard pressed to employ that option if the incident in question is a regional power outage and you have no generator. Will your security team act in different locations? If so, a single point of contact for documentation might not be the best option.

A cost-effective and oft-overlooked response technique is issuing pocket-sized pads of paper and training your personnel to write down the times events occur, response measures are enacted, and personnel contacted. Archaic might mean durable.

If your options include legal means of responding to an incident, good records are even more important: documentation is key to preserving the evidentiary trail in the event of legal procedures. Whether you rely on law enforcement or attorneys, the actual chain of events is crucial to your efforts; sometimes, the slightest misstep can guarantee the perpetrators' freedom and immunity.

Use of checklists and flowcharts can greatly expedite matters and maintain precision. Try to

brainstorm all contingencies, and tailor a set of responses for each. Have every member of your response team actually plot out, step by excruciating step, their part in a response: it's not unlikely that one or two key personnel might not be present the next time you have an incident, and knowing how to take up that slack can ameliorate aggravation, even if it takes more time. Checklists should contain the actual relevant phone numbers, e-mail addresses, and URLs for that response, and should be inspected and updated on a regular basis.

Notification

Depending on the nature of the incident, prompt notification of internal and external personnel may be warranted. This, like most aspects of security, is a precarious balancing act.

One of the industry-wide dilemmas for technology organizations concerns OPSEC- operational security. Who needs to know, and when do they need to know it? If your system is hit by a worm, for instance, is it in your best interest to alert others and risk further harm to your own system? Theoretically, in a cooperative environment, posting an indicator of the presence of malicious code assists everyone else in the industry by allowing them to block incoming attacks, spread the workload of definition resolution, and creation of patches. If followed uniformly, the tactic of "first-hit, first-alert" should encourage reciprocity and work to the betterment of the industry as a whole.

Realistically, the organization making such an announcement takes a number of risks. If the "attack" turns out to be a false alarm, the organization loses credibility (which can easily translate into a dollar value in the form of share price for publicly-traded companies and budget approval for government entities). Admitting a vulnerability invites future such attacks, and can garner press, which draws even more hacker/cracker attention. There is also the question of proportionality: if your organization is the first to make the statement that they're pulling the plug because of a particular incident, competitors who benefit from the early notification and aren't forced to react as dramatically can claim one-upmanship.

It is, by all accounts, a true Prisoner's Dilemma. All I can suggest is that you do what's best for your organization- report as early as possible. It is in everyone's best interest to do so. Relying on the security vendors is a dicey proposition.

Internal notification also involves some amount of risk. When reporting to your organization, keep threat advisory in proportion; causing undue alarm is just as dangerous as not eliciting

enough concern. Many systems professionals are quick to use shutdown procedures as the default response to any and all incidents ("an inoperative system is a safe system"). This tactic begs the result of such people being labeled the fabled Chicken Little or boy who cried "Wolf!", and can eventually breed mistrust and callousness to security policy and procedure.

Learning to minimize panic is a good recommendation for any security effort.

You might also want to decrease the frequency of attacks by taking pre-emptive steps to defuse potential attackers. A robust, dynamic security program can and should include active intrusion monitoring and detection; by contacting the owners of machines used to conduct attacks, oftentimes the attacks can be thwarted. Learn to look for intrusive patterns from sources with no reason to conduct such activities, and alert these organizations. Frequently, these entities are unaware their systems are being used for malicious purposes, as either wayward employees or third-party intruders using the devices as slaves are staging the attacks without permission or authorization.

You should also build communications channels with the law enforcement agencies that would respond to your incidents in the event they had jurisdiction. Contact your local authorities to determine to what extent they are prepared for systems incident support, not only from a criminal perspective, but including infrastructure concerns (i.e., what plans does your City Council have in place for disaster preparedness, who monitors and coordinates such events, etc.). On a national level, you have options in which agencies you utilize for reporting and response procedures. Industry entities are highly recommended: BugTraq, Trend, Symantec, SANS, etc. The FBI is also currently creating a cooperative framework of private and government organizations to expedite law enforcement, incident response, and prosecution efforts. Contact your local field office to find out more information about the Infragard program.

Investigation

Gathering as much information as possible within the time available is the best practice immediately following incident detection. Hasty decisions and uninformed reflex reactions are as dangerous as the causal incidents; in organizations that default to shutdown procedures, the threat of an incident has almost as deleterious an effect as the actual incident.

Logs and data collection are vitally important to your effort; having a machine-generated record of the actual times and transactions immediately preceding and after an incident occurs should

be one of your foremost goals in response. If you can afford to create only limited redundant systems, invest in those that will maintain an accurate timeline of events.

Try not to overlook any resources that might be at your disposal: even telephone logs can help you keep track of interoffice communication and rebuild the chain of events. Investing in cellular phones and pagers that annotate the time and number of each call is a wise strategy.

Interviews will also assist your response, both in preparing your list of eventual options and recreating the details of your efforts. While this process can be informal, it is best to remember that interviewing is one of the most difficult and misapplied techniques of gathering information.

Of foremost importance is the question of legal parameters: will this incident result in criminal proceedings or lawsuits? If so, it is almost certain that your interview process will affect the outcome. In the eventuality of involving law enforcement, it is best to forego any interviewing until the investigators are present, as this diminishes repetition, misconstrued intent, and the possibility that your efforts will impede proceedings. When lawsuits are concerned, wait until counsel is available to guide the investigation - attorneys will suggest lines of thought you might have ignored, and vice versa.

Of course, very few people are not intimidated and agitated when questioned by attorneys and law enforcement personnel (criminals, by and large, are among these). The timeliness of your response efforts will be greatly affected by this, as many subjects will want their own counsel present in such interviews, or refuse to participate altogether. Moreover, you will lose the greatest tool at your disposal when taking this tack: open and candid conversation.

If you opt to conduct interviews for the sole purpose of expediting response procedures and resolving the issue at hand, you should make every effort to engender a sense of mutual assistance and cooperation. Conduct your interviews in a completely forthright and calming manner, in a non-confrontational manner. This is extremely difficult, as the time factor involved with a response and the potential for embarrassing or bringing other harm to the subject is great. Try to explain that placing blame and administering punishment is not the ultimate purpose of the incident resolution, but organizational security; this tends to streamline and enhance the process of soliciting information.

Again, your best means for accomplishing this involve activity prior to an incident. Get to know the people in your organization, on both a formal and informal basis; security awareness and

training, office visits, and invitational functions are excellent opportunities to foster this relationship. At least let everyone know who your security personnel are, and what your intent is (security, not punishment). Ensure that your security policy hinges on open and honest user participation, as approved and reinforced from the highest echelons of your organizational structure.

Someone who inadvertently introduces an incident into your network will be nervous and fearful of repercussions: understand this. The few minutes you take to reassure the subjects of your interviews will save you hours in resolution.

In addition to interviewing concerns, when involved with legal matters in any way, all the data you collect can somehow be used as evidence. Discuss the proper procedures for collecting and preserving the data with law enforcement and attorneys to ensure compliance with local statutes and best practices. Moreover, your responses are limited by law as well: seizing someone's workstation, magnetic media, and other belongings might not be condoned in some circumstances. Be aware of those limitations before acting.

An Example of a Response

ASSUMPTION: The preceding paragraphs should emphasize the need for tailoring your response procedures to your unique requirements. This example is offered solely as a possibility for a feasible response effort, not a panacea model.

While monitoring intrusion event logs at 2:00 a.m., personnel in the organization's 24-hour network operations facility discover a successful attack has occurred.

For many organizations, the immediate response would be to disconnect the network to retard further exposure and contamination, but we're trying to avoid knee-jerk overreaction, and the monitoring personnel are aware of this. Instead, they run the checklists already in place to cover this type of event.

The first step is to notify and brief the head of systems security (or their proxy, whichever is on call). It takes a few moments to rouse this person and get a lucid acknowledgment, but eventually the situation is made clear. Four minutes have elapsed since the initial notification.

With what information is available, the security representative declines to opt for full system

shutdown, but authorizes a response team recall. The monitoring personnel run the recall checklist while the security representative travels to the workplace. Representatives from the organization's networking operations, legal, engineering, administrative, and management sections are all notified and requested to return to the predetermined location. Local law enforcement is notified, and a timeline of events opened.

28 minutes have now elapsed from the time of initial notification.

The security representative, being the first contacted, is the first to arrive. This person commences response center setup and preparation. The contingency bag is unpacked, revealing a laptop, AC and car adapter jacks, extra batteries, lamp, toolkit, checklists and notepads for all members of the response team, portable printer and a ream of paper, a cellular phone, first aid kit, and other sundry items. (In most organizations, the person on the scene will also make the first pot of coffee). Copies of the information available to this point are also prepared for distribution to team members and senior management staff at this point. 57 minutes have elapsed from the time of initial notification.

Other team members arrive sporadically during this time, and the monitoring personnel have conducted further research into the intrusion. Preliminary investigation reveals that the intruder has breached one user's workstation, but has not yet progressed to other points in the network; the attack was engineered through the user's employment of an unapproved dial-up connection. The actual intrusion took place eight hours before initial discovery.

The full team is assembled 92 minutes after initial notification. All members are brought up to speed on the situation, and begin brainstorming options and tactics. Discussion gives way to concurrence: the affected workstation will be taken off-line, and containment and identification efforts commence. A briefing is prepared for senior management, and the initial steps are completed. 108 minutes have elapsed.

The network operations representative is dispatched to disconnect the workstation. The administrative representative updates and rechecks the timeline on the laptop; this person will now serve as the focal point for all team communication and activity, keeping a running record of all events. The legal representative, having been made aware of the situation and offered guidance, returns home with instructions to return at start of business that morning. The engineering and security personnel inspect the information gathered thus far, including the data from the affected machine; this is studied on a standalone testbed network, and analyzed to

identify the attacker, the means of attack, and possible ways of patching the vulnerability organization-wide.

With 141 minutes elapsed, the team reassembles to review and update progress. It's been determined that the attacker used a spoofed foreign IP through a dial-up connection, and - evidently- was only able to access the single machine. A thorough check of the network will require that the servers be taken offline, effectively halting operations for six hours. The team, pending legal advisement and senior management approval, elects to perform this sweep, but only after close of business later that day.

When the workday begins, more activities transpire, including an interview of the user whose machine was penetrated, sanitization of the affected system, and briefing senior staff, but for all intents and purposes, the response has climaxed and resolution begun. By 11:00 p.m., the incident will be resolved and the final report will be filed the next day.

There are those who insist on the immediacy of the threat predicating an instantaneous action for containment, and the two-plus hours might seem to them an unnecessary and foolhardy waste of time; for your organization, this might be the case, and you want your first step following identification to be abrupt and unilateral isolation of the network and system(s). On the other hand, in this particular case, the advantage of methodical procedure was the preservation of normal operations for an entire workday; instead of shutting down the entire organization's system for a whole day, the result is a half-dozen tired people, a few hours of compensatory and overtime, and one system down during the workday. The dramatic cost saved by this effort was deemed well worth the risk by those involved.

Ben Malisow is an INFOSEC policy analyst for a Department of Defense contractor in Virginia. He received his B.Sc. from the Air Force Academy and recently completed his MBA. Currently Ben is a political columnist for a Washington, D.C. newspaper and senior editor for a humor website.

Relevant Links

[FedCIRC](#)

Federal Computer Incident Response Capability

[DoD-CERT](#)

Department of Defense Computer Emergency Response Team

[AFIWC](#)

Air Force Information Warfare Center

[NSA/CSS INFOSEC](#)

Information Systems Security Organization

[FIRST](#)

Forum of Incident Response and Security Teams

[CERT](#)

Computer Emergency Response Team

[Privacy Statement](#)

Copyright 2006, SecurityFocus