

Thousands of Products,
Hundreds of Dealers,
Virtual Trade Show,
Much More!
Processor.com Home

 [Email This](#)
 [Print This](#)

Search Past Articles
All Tables Of Contents
Cover Focus Articles
Tech & Trends
New Products
Product Releases
MarketPlace News
Factoids
Opinions
MarketWatch
Book Reviews
What's Next
What's Happening
Upcoming IT Events
The Latest Versions
This Week's Issue

Cover Focus Articles

General Information

March 4, 2005 • Vol.27 Issue 9

To Catch A Thief

Steps to Help You Prepare To Conduct Incident Response & Forensic Analysis



Responding to computer or network security incidents requires some advanced planning and preparation. It is important to have a clear understanding of what the goal is before you begin performing any incident response or forensic investigation. It is also imperative to consider any legal or regulatory implications to ensure that your incident response is in compliance and doesn't expose the company to any legal or financial ramifications.

Harlan Carvey, author of "Windows Forensics and Incident Recovery," says, "If a company or organization handles any sensitive or critical data at all, it must have an incident response policy."

Chris Davis, Aaron Philipp, and Dave Cowen combined their extensive knowledge of incident response and computer forensic analysis to author the book "Hacking Exposed: Computer Forensics." They believe that it is necessary for companies to create a defined incident response policy, as well. "Ad-hoc investigations do more harm than good. Investigations can originate from human resources, system administrators, the ethics hotline, physical security, managers, internal audits, external audits, other internal parties, and forces outside the company. With so many origination points, a process needs to exist that clearly defines how to handle the broad spectrum of cases and people that may be involved in an investigation. The policy provides guidance as to where to funnel the investigation and to difficult decisions such as how to handle critical systems."

As with disaster recovery and business continuity, companies must consider what impact a computer security incident might have and how they choose to respond before the incident occurs. Having developed a well-thought-out plan in advance will not only make the incident response process smoother and more efficient, but it will also lend credibility to any evidence collected and make it more likely that the data will be admissible in court if it comes down to that.

■ Defining A Plan For Incident Response

According to Davis, Philipp, and Cowen, there are three major things that companies must do when defining how they want to respond to security incidents:

- Decide whether there is any intent to prosecute the attacker

- Create a defined process and written procedures for incident response
- Understand the legal and regulatory ramifications that apply to them

Network administrators are frequently caught off guard when a security incident occurs and they have no defined means of responding to it. Should the system be taken offline? Should the system simply be rebuilt from scratch and put back online? Should research be done into how and when the incident occurred? What tools or utilities should be used to do the investigation? Will the data collected need to be used as evidence in court proceedings? By the time the network is hit with a security incident, it is too late to properly consider all of the appropriate questions and respond to them accordingly.

Carvey says, "I've worked for companies with no incident response plan, and the IT department actually created incidents!" He continues, "The first step is to decide what, if anything, they want to do in the event of an incident. This may necessitate changes in their infrastructure as they make things more manageable and increase their incident prevention posture."

Davis, Philipp, and Cowen add, "The decision to prosecute determines how you handle the evidence. This may not be important in the mind of the system administrator, who is more concerned with who and how, but the overall company is taking a risk when it decides to examine a system without a coherent plan."

■ Throw The Book At Them

If the decision is made up front that the company wants its incident response policy to allow for the possibility that the data collected might need to be used as evidence to prosecute legally, there are a couple of key steps that should be taken.

Davis, Phillip, and Cowen say, "Most cases in a corporate environment are on someone's laptop or computer under their desk. Instead of browsing through files on the live computer, the manager or someone delegated should remove power without shutting the computer down. Pull the plug."

They continue, "Few attackers leave no trace of themselves in the system logs and fewer still manage to keep all of their tools loaded in memory only. Once the system is offline and an image of the system is created from tools such as dd, SMART, or Encase, you can begin to evaluate the computer's hard drive."

In many cases, though, companies simply don't have the resources to follow through even when they have a defined incident response plan. Carvey explains, "Far too many times data is collected, but nothing is done with it. There is often not enough time or the person performing data analysis doesn't have the necessary skill sets to actually perform analysis. What happens then is that the root cause analysis or determination of what happened amounts to nothing more than unfounded speculation."

■ Fill Your Forensic Response Toolbox

There are a number of tools and utilities available to help you perform a forensic analysis of a computer system and conduct an investigation of a security incident. Which one should you use?

There is no right answer to the question. The OS platforms you are familiar or

comfortable with, as well as which platforms you will be conducting analyses on, may steer you to one tool or another.

Carvey suggests EnCase from Guidance Software. "It's used by law enforcement, and when many of the folks who use it move on from law enforcement functions and into the civilian world, they take that preference with them. Other products, such as FTK, Autopsy/TCT, and FLAG seem to be used to an extent, as well." He continues, "A company needs to look at its requirements and policies and then choose the best product or products to suit its needs."

Davis, Philipp, and Cowen agree. "Do you plan to do your investigations internally? Do you have a sharp Linux staff? If so, then consider a tool such as SMART from ASR Data. If you're more comfortable with Windows, then consider Encase from Guidance Software."

They also point out some other factors to consider when selecting tools for your forensics toolbox. If you are going to need to analyze enterprise mail stores or large database files, there are tools geared toward these tasks. If you have a lot of mobile devices, such as PDAs and cell phones, that may need to be analyzed, they advise using Paraben, a leader in the mobile devices market.

The best advice these computer forensics experts have to offer though is the following: "Forensic tool providers are striving to provide the one-stop solution, but it doesn't exist. Every company and case is different, and your toolkit has to provide you with the capabilities you need to make your response and investigation a success. Only by determining what your needs are can you pick the tools that will help you do your job."

Regardless of whether your incident response plan will include the possibility of legal action or simply provide some peace of mind to administrators and management that the incident has been handled, answering questions in advance about how an incident should be handled and clearly defining the procedures to be followed will help make any incident response and recovery go smoother and more efficiently than just winging it. ■

by Tony Bradley

[View the chart that accompanies this article.](#)

*(NOTE: These pages are PDF (Portable Document Format) files. You will need Adobe Acrobat to view these pages. **[Download Adobe Acrobat Reader](#)**)*

[Return to Previous Page](#)

[Home](#) **[Copyright & Legal Notice](#)** **[Privacy Policy](#)** **[Site Map](#)** **[Contact Us](#)**

Search results delivered by the Troika[®] system.

Copyright © by Sandhills Publishing Company 2005. All rights reserved.