What Went Wrong?

And How Could It Have Been Avoided?

by Christoph Fischer (fischer@bfk.de)
and Kenneth R. van Wyk (ken@krvw.com)

Abstract

In this paper and accompanying presentation, the authors draw on their collective experiences in the field of Incident Response and provide a series of case studies and lessons learned. In presenting and analyzing numerous incident case studies from the academic, military, and commercial sectors of Europe and the USA, they provide a critical analysis of the mistakes that were made. The flaws uncovered here include technical as well as procedural shortcomings.

Case Studies From The Trenches

Each of the stories below represents the authors' factual depiction of the events that took place during an actual incident. The identities of the organizations involved have been removed, but the stories are otherwise retold in as factual a manner as possible. That said, what is presented here comes from the authors' memory.

It's an IT Problem

In one financial services firm, the IT Security department was tasked with drafting an incident response plan. They did, but the resulting plan was—as one might expect—rather "IT centric". Although it paid thorough attention to technical details and issues, it didn't account for any resulting business impacts. Disaster was averted during a live incident, but the case really illustrated the importance of placing the business priorities first and foremost. When faced with having to respond to an incident, the drafted process would have failed if the personnel involved did not circumvent it and approach the business owners first.

Lessons learned from this incident include the following:

- Although in many smaller organizations, the IR planning is often done by the IT staff, it needs to be clearly understood that a security incident is a business issue, not (just) a technical one.
- The decision flow of the IR process should be (and was) revised to start with the business owners first to set the strategic business priorities in resolving each incident. Once decided, the IT staff develop a technical/tactical course of action that best represents the business priorities.
- Always include the business process owner(s) in the planning phases of developing an IR capability.
- This type of planning flaw could well have been isolated and fixed prior to an incident by running a realistic exercise and putting the draft process to the test.

On Trusting Trust

In the pre-rootkit days, an IRT had keystroke-level logs of an intruder breaking into a system at one of its facilities. When sent to investigate, the IRT staff used the tools available to them on the compromised system, only to discover that nothing seemed to have been touched. Indeed, event logging during the hours of the (presumed) intrusion were blank, and the directories deposited by the intruder were not present. It turned out that an early rootkit had been planted on the system. These days, rootkits aren't out of the ordinary, but the importance of this incident was that the IRT personnel had based their trust on false assumptions—something that can easily happen in the “heat of battle”. It is vital to keep focused on the task at hand and to have a “big picture” view of the actions being taken so that each and every assumption can be appropriately questioned.

Some of the lessons learned during this incident include:

- It's easy to look back at this incident and say that the IRT personnel should have been more careful about which tools that they used. Understand, though, that no rootkits had yet been observed in actual incidents. Nonetheless, faced with the clear discrepencies between the different data, they should have dug deeper.
- Rootkits are, of course, quite common these days. Let's use this lesson to ensure that we're prepared for the next big thing in attack tools. Be cognizant of your assumptions, decisions, and the ramifications of each. Booting a server farm from trusted boot media may not be a feasible option, so how can you ensure that your tools are telling you the truth? To what extent should paranoia be taken?

Shipping Monitoring Equipment

In one spectacular failure, an IRT was called on to respond on-site to a major hacking incident. A tool box full of evidence/data collecting equipment, software, etc., was rapidly assembled and arrangements were put in place to “airport-to-airport” ship the tools to the location where the IRT personnel were traveling to. The only problem was that the airline somehow lost the box. In a classic case of putting all of one's eggs in one basket, the IRT personnel were all but incapable of doing anything productive for approximately 24 vital hours. While it's easy to look at this story and say, “how on earth could they have been so stupid,” it's much more important to put together logistical plans that anticipate failures. After that mistake, the IRT made a point to always take at least a minimal set of tools in carry-on luggage. In the post-September 11th era, though, how much can be reasonably expected?

Some of the lessons learned from this painful episode include:

- Never ever ship critical equipment to an incident site.
- Embrace redundancy in IR equipment. That is, ensure that each component can perform multiple functions and act as a backup for other tools, if necessary.
- Pack lightly. When traveling to support an IR operation, use the smallest equipment that can feasibly do the job at hand. Distribute the equipment among the team members and keep the equipment as carry-on luggage.
- If it is absolutely essential to check-in or ship equipment, make sure that the function can be performed by other equipment that is being carried.
- Arrive very early at the airport and be excruciatingly cooperative with the airport security personnel.

Maintaining Chain of Evidence

An IRT was called to assist a client in the entertainment industry after one of its employees discovered a possible insider-misuse hacking situation. In the hours that it took for the IRT to arrive at the client's facility, the suspect was interviewed by management and by the Human Resources department and given the option to resign from the company rather than face potential charges. Although this may have been an appropriate step, what followed wasn't... They allowed the (by now former) employee to return to his office, collect his personal belongings, and leave the building—unescorted. Without realizing the ramifications of their actions, they placed the company at great risk and likely damaged the evidentiary usefulness of any information subsequently collected. Although no damage is believed to have occurred, the situation illustrates the importance of handling information (and former employees!) with great caution.

The important lessons from this incident include:

- Treat all information in an IR operation as though it might be needed for evidence; that is, follow strict 2-person rules (depending upon your local law enforcement rules of engagement). Do this until and unless the incident is thoroughly evaluated and the appropriate decision authority decides that no evidentiary procedures will need to be followed.
- Ensure that all Human Resources processes include guidance for appropriate evidentiary handling for such an incident. Never leave an employee who is being terminated *for cause* alone with any company IT assets.

Embarrassed Customer Tells Only Partial Story

The web server and the firewall of a compromised site of a large industrial corporation were both 'homegrown' and in an incredibly bad state of disrepair. To make matters worse, the system administrator's conscience even drove him to cover up some of his own shortcomings, keeping some of the details of the incident from the company's IRT. As a result of this, a group of attackers noticed that they had been detected and never returned. The administrator made several changes to the system and its configuration. He also reset the CMOS clock without noting down the skew it had, which lead to a very confusing and difficult forensic task. Fortunately, the attackers made a few mistakes of their own that finally lead to enough evidence to get a court ruling for a wiretap and resulted in 14 arrests.

Lessons learned, that could have saved tons of time:

- The primary lesson here is a time honored one: trust but verify.
- Interviewing of involved parties *is* a valid method in dealing with incidents, *but* always double check what they tell you.
- Make sure the people view you as a consultant that helps them fix a problem and not as someone that is going to report everyone's shortcomings to management after an incident. Don't underestimate the value of a cooperative and supportive team spirit during an incident.

Dealing With Law Enforcement on an International Basis

During an incident involving a group of attackers from another country, using intermediate victim systems in the IRT's home country as well as elsewhere around the world, the process experienced numerous interesting and unexpected delays. First off, way too many entities were involved in relaying vital information, which caused major delays in addition to distortion of the content. Also, country specific issues like Italian office hours (long lunch) and US priorities during a national holiday (Thanksgiving) led to confusion and potentially threatened the success of the operation. The incident did draw to a successful closure, but the situation really highlighted some of the entirely non-technical difficulties that one faces in dealing with an incident of such a massive multinational extent.

Lessons that could have cut the international phone call bill in half:

- When dealing with entities in other countries, never assume that things will work the way you are used to. Be cognizant of other countries' customs, holidays, etc., and work around them.
- Timezone, language issues, and legal systems are very evident differences, but cultural differences can play an equally important role.

Rules are meant to be broken.... and will be broken

During the task of analyzing evidence in a case, a former employee was accused of planting a virus in his company in response to the termination of his employment. The IRT was supplied with a box full of floppy disks to analyze and store as evidence. They used a vault to store the originals and performed the tests on images. Extreme care was taken to apply the rules of chain of custody for these pieces of evidence. During the court hearing, the question was brought up why the material was not marked with a evidence code stickers. It eventually turned out that the police officers had no experience in electronic evidence handling, and had stored the diskettes in a simple cardboard box in their office for several months. When the case was handed to the prosecutor, they had to search for the box for several days. Then, exacerbating the problem, the prosecutor moved office shortly after taking over the case and the very same box was 'lost' once more for more than two months. Luckily, there was enough information on the floppies to convince the judge to admit the material. Among the stuff were scripted login procedures that revealed user id and password in clear.

Almost amusing how much can go wrong:

- Never assume that things work they are intended to work.
- When handling evidence, be pedantic in every detail. In some countries, a mistake like this would have resulted in having the evidence declared inadmissable.
- There is a reason for everything like the missing stickers. Ask and document!