Incident Response and Digital Forensics: Will You Buy or Build?

June 6, 2018 | By Warren Perez Araya | 3 min read

Bigstock

When thinking about digital forensics, most people imagine a court and lawyers. But this isn't true in most cases, as it's much more than legal processes or procedures. Forensics is essentially the process of understanding why, when and how something happened. This could be done for a criminal investigation, a civil investigation or just as an internal incident response (IR) investigation.

It's difficult to guess when an incident is going to occur — and

a court of law.

Companies must be prepared to respond if something unexpected happens. Generally, organizations have two options for IR and digital forensics: Buy or build?

Buying Incident Response and Digital Forensics

What does it mean to "buy" an IR and digital forensics team? It's simple: A company pays another company to support them in the event of an incident. There are several advantages to this type of service. For instance, the company does not need to invest in equipment and personnel, as the service provider provides everything. The IBM X-Force Incident Response and Intelligence Services (IRIS), for example, offers teams to clients who've had a security incident.

Services provided by IRIS include:

- IR planning
- Remote threat response
- On-site incident response
- Around-the-clock access

Of course, this doesn't mean that a company using this type of service doesn't have to do anything in-house. The internal personnel must be trained in IR on a fundamental level. This would be like training your staff in first aid — they don't need to be experts, but they should have at least some basic knowledge of how to act in an emergency.

role. This person will be in charge of contacting and engaging the on-demand IR team. Evidence must be preserved, and a trained staff member should be in charge of ensuring that happens.

Building Incident Response and Digital Forensics

The second option is to build your team. This means investing in qualified and trained personnel, equipment, tools and a laboratory. It's not every day that a security incident needs to be investigated from a forensics perspective — but when the time comes, it's always better to be prepared.

There are several types of investigations that you must consider when building an IR team. When investigating an internal incident, the chain of custody is not that critical. For instance, if the IR or digital forensics team has to engage with a possible virus infection, the most important thing is that they secure the infected machine or machines. This allows the team to start working with the secured devices and analyze the software and look for indicators of compromise (IOCs). How the evidence is collected is not vital in a scenario like this. However, if the investigation must be presented to a court of law, how the evidence is collected and secured is vital.

Understanding this, an on-site IR team can be built to match what a company really wants or needs. Perhaps the noncriminal or civil investigations would be handled by the on-site team and the rest by a third-party company. Maybe the company wants to have a team capable of dealing with all sorts of investigations instead, which requires legal advice, a larger team and a lab to meet standards for compliance.

or a contracted team encounters child pornography, all tasks being performed must be stopped. The area must then be secured and any person that interacted with the device (computer, cell phone, server, etc.) must stay where they are until the authorities are called and arrive at the scene.

Making Your Choice

The decision to either buy or build an IR and digital forensics team boils down to two questions:

- What do we want to respond to ourselves?
- What is our budget?

Answering the first question can give you an idea as to whether you need a team capable of adhering to the lawful way to collect evidence or not. The second question is the tiebreaker. Building an IR team and equipping the team with the necessary tools and infrastructure could be more expensive than contacting these services from third parties — having the trained personnel, or training (if needed), costs money.

A company could transfer those expenses and the risk of having an on-site IR team by contracting these types of services with a team of specialists. In the end, answering these questions can give you an idea as to the right option for you.

Tags: Incident Forensics | Incident Response (IR) | Incident Response Plan | Security Services

Warren Perez Araya

SIEM Admin, IBM

Warren Perez Araya is a contributor for SecurityIntelligence.

More from Incident Response