How Do You Define Digital Forensics in the World of Cyber Security?

Bob Osgood

The cyber security industry is fascinating for several reasons. First, everyone is affected since everyone in the industrialized world has/uses computers and mobile devices. Second, no one seems to get it right. This is not a knock on anyone, just an observation. Why, because people love the freedom and functionality that the digital world provides, but cyber security is annoying. Without the digital world, working from home would not be possible.

Cyber security is like blind person touching an elephant. You only see it in terms of what can be touched directly in front of you. If you talk to cyber security developers, they will focus on the latest and greatest algorithms to detect and deter ransomware. Talk to information systems security officer, and she/he talks about access control lists. Human resource security professionals focus on policy; what employees are allowed and not allowed to do.

The Chief Information Security Officer, aka CISO, is worried about everything because the next breach could be an employment ending event. Notice I said the next breach, because that CISO got their job because of the prior breach that occurred. The average life expectancy of a CISO is 26 months.[1]

Attorney's are concerned with legal liability that will arise as the result of a breach, and the Chief Financial Officer is concerned about if the organization has enough breach insurance.

Ransomware attacks and breaches by advanced persistent threat organizations are on the top of everyone's list.

Cyber security and digital forensics overlaps considerably. Why, because when your organization gets compromised, it's the digital forensics examiner/analyst that will figure out what is going on.

Before the Breach

Before your organization is compromised, conduct a detailed analysis of your cyber security posture. Some call this a cyber risk analysis. Figure out what digital assets you have, what digital assets need to be protected, and then decide what you are going to do to protect those assets. A few things to consider:

- Multifactor authentication
- Encryption
- Network segmentation

Now there are many other things to consider, but I consider these to be the big three. Why, because if you have these three figured out, the others will fall into place. A few other things to consider:

- Off-line backups
- Logs – logs – logs

[1] https://www.zdnet.com/article/average-tenure-of-a-ciso-is-just-26-months-due-to-high-stress-and-burnout/

- The management of users
- Edge protection
- User training

Before we go any further, I need to point out that no operating system is immune to attack, and what is your organization doing about mobile devices used on company networks?

Ok, let's take these things[2] one at a time.

Multifactor authentication, something you have and something you know, is an effective security authentication practice. With the advent of mobile device applications (e.g. Duo), implementation is much more manageable than the day of key fobs. What two factor authentication gives is protection over the compromise of a username and password. This happened to me a few years ago. Attackers compromised my username and password on a sensitive system, but when the attackers attempted to log in, I got two factor confirmation alert and was able to stop the compromise. I immediately reset my password and alerted network security. Network security was able to track the attack which originated in Africa but was bounced through a university in Florida.

Encryption generally doesn't prevent compromise, but it does prevent theft. What I mean here is encryption at rest. So, data/files/stuff stored especially on file servers needs to be encrypted at rest. When your file server gets compromised, and data gets exfiltrated (aka exfilled), the attacker has nothing.

Network segmentation is breaking up your organizations network into smaller logical networks called subnets. This can be done through the use of virtual local area networks (VLANs) or by breaking up your network by IP blocks. The reason for doing this is simple. Does the mail room need access to computers in the marketing department. Do the salespeople need access to computers in the research department? By breaking up your network, you are making the ability of the attacker to move laterally in your organization that much more difficult.

Offline backups are probably one of the best defenses against ransomware attacks. When you fall victim to a ransomware attack, having uninfected backup goes a long way to recovering. A solid backup scheme is not a sexy thing that anyone wants to talk about, but it can save your bacon.

Logs – logs – logs or document everything. The better your record keeping system, the better you will be able recover from any compromise. Maintaining a separate logging server where as many as logs as possible can be stored is highly recommended. You will need to manage this data so that it is easily retrievable and well secured. Just dumping files onto a disk is a recipe for failure.

Properly managing users sounds simple, but in large organizations this can be a challenge. A good identity management system goes a long way here, but at a minimum, user access needs to be reviewed regularly. What does regularly mean is up to some interpretation, but at a minimum at least once per

[2] This is a technical term.

week. This review will entail matching users to their current H/R status focusing on terminations/suspensions/transfers, etc. A red flag needs to be raised if there is a user account that does not map to a current employee.

Edge protection is also not one of those sexy topics. Everyone expects it to be there, but how and to what extent edge detection is deployed varies. Edge detection involves the use of access control lists (ACLs), intrusion detections systems (IDS), and intrusion prevention systems (IPS). Deploying effective edge protection is not trivial, and there are a plethora of options. There are also specialty products in the market. One example is RansomGuard™[3] which is an endpoint File Integrity Monitoring (FIM) tool which utilizes deceptive defense. It is designed to feed logs directly to existing SIEM solutions such as Splunk. RansomGuard™ comes with several capabilities beyond simple FIM and can react to situations such as data exfiltration depending on customer enabled settings. Users can choose to have RansomGuard™ more proactively intervene when it detects file changes, such as logging behavior and then shutting down the host system. RansomGuard™ is a ransomware mitigation tool.

User training is last on our list, but it's in no way the least. Training users to spot phishing attacks goes a long way to minimizing your threat landscape. Some organizations have gone so far as to test users with faux phishing emails. When (I say when because some dope is going to click on this) a user clicks on the faux message, they are alerted that the email was a faux phishing message and then directed to take some training. Research that I've seen reveals that most employees learn from this experience, but there will be a few holdouts that will never get it. What if one of your holdouts is the CFO?

Where does the digital forensics stuff come in?

OK, so your organization seamlessly integrates all of these cyber security technologies, processes, and procedures flawlessly. Are you out of the woods? No, but your recovery time and loss risk are reduced significantly. When you do get compromised, your response will depend on your digital forensics capabilities. These capabilities can be inhouse, external, or a combination of the two.

Before we get into individual skillsets needed, we need to address evidence collection capabilities. Yes, I use the legal term evidence here because there is always a chance that some court of law may get involved although, generally speaking, the odds are low that your breach investigation will ever see the inside of a courtroom. Remember, it's better to have it and not need it, then to need it and not have it.[4]

Collecting vital evidence is crucial to analysis. Such evidence includes logs (see above), memory snapshots, selective artifact extraction, and only if absolutely necessary drive imaging.[5] Selective artifact extraction is extremely comprehensive. This article won't cover all of them, but the highlights include volatile data, selected non-volatile data, and memory snapshots. Non-volatile data includes logs, file listings, IP addresses, Prefetch, Pagefile, system Info, browser cache, etc. Volatile data includes running processes and services, open and listening ports, arp cache, dns cache, etc. Telemetry from your IDS and IPS systems is also desirable.

---

[3] RandsomGuard was developed by Mason grad and adjunct professor Gordon Long.

[4] Alien vs. Predator, 2004.

[5] Drive imaging is a laborious process that usually doesn't produce anything usable in a timely manner.

Digital forensics examiners/analysts come in many shapes and sizes. Digital forensics collection and analysis skillsets include:

- Digital Media
- Memory
- Network
- Cloud
- Mobile devices
- Reverse engineering

Any and all of these skill sets may be invoked in a breach. Where the examiner/analyst starts is usually from an alert or report from a user. Alerts come from IDS/IPS's or antivirus package. A user can report a malfunction or some anomalous activity that turns out to be evidence of a breach. Another possible way to be alerted, but not the best way, is when the FBI or USSS knocks on your door.

Digital forensics as a discipline came from law enforcement. Once computers became commonplace (early 1980's), criminals starting using them for evil purposes. Mobile devices (aka cell phones) became ubiquitous in the 1990s and guess what, bad guys used them in fact loved using cell phones. Malware, programs that do things that you didn't pay for, generally requires reverse engineering. The Cloud is essentially using somebody else's computer. Gee, criminals do that all the time. All these computers communicate via the Internet. So, knowledge of networks is critical.

Conclusion

Even the best cyber security system will eventually be overcome. When that happens, you need to be in a position to collect the evidence necessary that digital forensics examiners/analysts can use to effectively figure out what happened, stop the bleeding, and remediate the problem.