LBMC Information Security Cybersecurity Sense Podcast Show Notes
Author: Bill Dean
Episode: 29
Date: August 15, 2018

Incident Response Should Be Common Sense

Article: Addressing Incident Response with Some Common Sense

- To give full credit, the base for this podcast comes from an awesome article written by Kevin Beaver for toolbox.com. After leading incident response practices for about 10 years, he does a great job of summarizing many situations.
- Let's be honest, no one desires the experience of an incident. That is likely why organizations do not plan for an incident by creating their incident response teams, creating incident response plans, or testing their capabilities. This is likely why most organizations are caught off guard when they experience an incident. And, all organizations will have an incident at some level. Responding to an incident does not have to be as complex as we often make it. It is all about what happened, how did it happen, when did it happen, and what data was at risk? When we have figured that out, let's get back to what we do best.
- It is important to stress that incident response issues are no longer just an IT issue for the organization, as legal issues are often involved. Everyone has data of value, that is why the organization was targeted (PII, EPHI, Credit Card Data, Financial information, etc.). The implications of a breach of these types of information are beyond concerns only within the organization involved. The complex matrix of disclosure laws are often involved.
- To endure your incident, you need to focus on certain things.
  - Develop your incident response team. This isn't 2002, and incident response is no longer just an IT issue. You will need the IT expertise. But, you also need management, legal, HR, PR, etc. on your team. In developing your team and plan, a crucial aspect is who can/will make decisions?
  - Clearly define an "incident." What are the differences between "events" and "incidents."
  - Do you need third-party resources, such as incident response expertise, outside legal counsel, public relations, etc.? In other words, who would you need to contact? Make that list on your plan. If you hear nothing else from this podcast, get these needed folks on retainer before you have an incident. When the incident is in progress is the worst time possible to create these relationships from both a pricing and procurement perspective.
  - What tools and data sources will you have available to investigate (SIEM, NETFLOWS, LOGS, Malware alerts, etc.)? Incident response is often about "proving the negative." Do you have what is needed to do that? If not, work on that now.
  - Does your plan work, and do you have the evidence sources needed? How do you know? Have you tested the plan and confirmed that the data sources exist?

Key Takeaways:

- A computer security incident is something that no one wants to endure. However, there is some certainty that you will experience one to some level soon.
- If you plan accordingly, working through an incident does not have to be “black magic.”

Action Plan:

- If you do not have an incident response plan/program, you need one. If you are not comfortable creating that, find someone who can.
- If you have not tested the plans involving people, policies, and technologies, you need to. If you need outside help, find it.
- This is your opportunity to test yourself and make decisions to execute during an actual incident. The incident is coming, and you can prepare now.

References:

- https://it.toolbox.com/blogs/kevinbeaver/addressing-incident-response-with-some-common-sense-071118

Bill Dean is a Senior Manager at LBMC Information Security. While involved in various aspects of LBMC’s security services, he is also the practice lead for the organization’s incident response, forensics, and litigation support practice.