Breaking Down What Incident Response Means for Your Business

The Need for An Incident Response Plan

In today's world, Cyber-attacks are becoming the norm. Not one business or corporation is immune to them. It seems that no matter what an entity does to fortify its defense perimeters; the hacker will find a way to circumvent it and inflict as much damage as they can. There are no geographic or industrial constrains, anything and everything is fair game, as the following examples illustrate:

Consider the following statistics:

- It was discovered that there was a major security vulnerability in Cloudflare. This was a buffer overflow weakness, which resulted in the compromise of the confidential and private information of end users from 3,400 websites. This included the likes of Uber.
- Edmondo is an organization that specializes in educational technology, and they are based out of California. They were the victim of a Cyber-attack that resulted in in the compromise of 77 million end user accounts, and these were available on sale for $1,000 each on the "Dark Web".
- McDelivery is the mobile app for the McDonald's franchise in India. Because of a vulnerability in its public API, Cyber attackers were able to hijack the private information of over 2.2 million customers, which included e-mail addresses, phone numbers, social media profiles, and even residential addresses.
- Melbourne IT, an Australian based Internet Services Provider, was the victim of a major Distributed Denial Service (DDoS) attack. Because of this, their servers went down for 1.5 hours, afflicting such services e-mail, web hosting, and control panel access.
- The E-Sports Entertainment Association League, is a video gaming company based out of Germany. They were the victim of a Cyber-attack, which resulted in the compromise of at least 1.5 million end user accounts.
- Cellebrite is a major forensics firm based out of Israel. They too were a victim of a major security breach in which 900 GB of customer data was covertly hijacked.

(SOURCE: http://thelibrary.solutions/library/newsletters/2017-cyber-attack-trends%20Mid-Year%20Report%20(EN).pdf)

The Incident Response Process

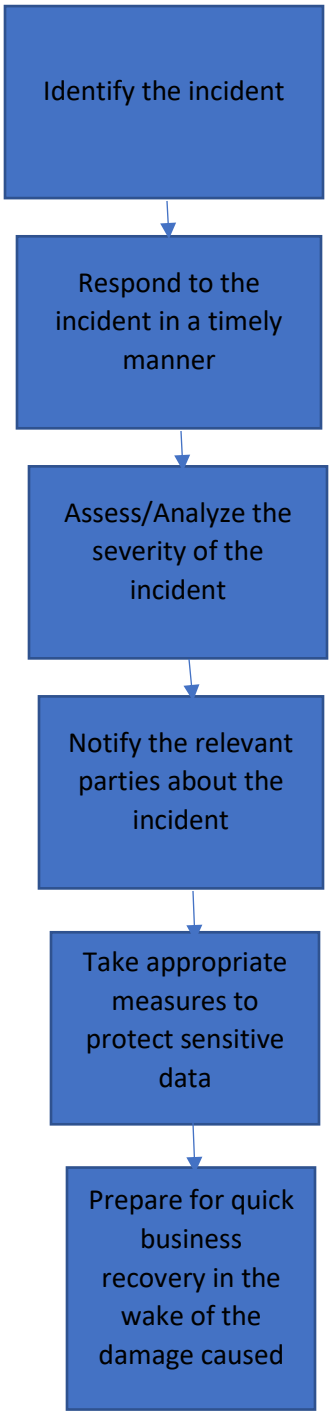
The unfortunate truth is that many cyberattacks are so stealthy that they often go unnoticed for a long period of time. This is where Incident Response (IR) becomes absolutely critical. It can be defined as follows:

"The process by which an organization handles a data breach or cyberattack, including the way the organization attempts to manage the consequences of the attack or the breach. The goal is to effectively manage the incident so that the damage is limited in recovery time, costs, and brand reputation".

(SOURCE: www.digitalguardian.com).

It is absolutely crucial to respond to an incident as soon as it has been discovered. The above definition states that a process must be used, but it must be an orderly one.

The IR process must detail how to handle just about any type of cyber-attack. It must be viewed as an emergency plan in order to increase the chances that a business entity will be able to resume normal operations quickly and efficiently. This process can be diagrammed as follows:



The Benefits and Needs for Fast Time to Detect and Time to Respond Periods

When an organization is hit by a cyber-attack, the IT staff obviously needs to respond as quickly as possible to the incident. Any wasted time will translate into more downtime in the end, which will mean lost revenue, damage to brand recognition and, worst of all, lost customers.

There are numerous benefits to responding as quickly as possible to a Security incident, some of which are as follows:

1) Downtime, if any, will be minimized.
2) Quickly responding to a Cyber-attack and immediately notifying customers as to what happened could, in the long run, actually win new business.
3) Showing your insurance agent that you responded quickly to an incident by having a well-crafted Incident Response Plan will not only mean that you will receive your claim payment quicker, but you could also receive policy discounts in the future.
4) Timely response to any kind of security breach allows for a thorough investigation to follow in an expedient fashion.
5) Responding quickly to a Cyber-attack will create a proactive security mindset among the employees in any organization, large or small.

The following matrix illustrates who should be involved in responding to an incident:

Team Leader	Responsible for the overall incident response; will coordinate the necessary actions that need to take place.
Incident Lead	Responsible for coordinating the actual response.
IT Contact	Responsible for communications between the Incident Lead and other members of the IT staff.
Legal Representative	Responsible for leading the legal aspects of the incident response.
Public Relations Officer	Responsible for protecting and promoting the image of the business entity during an incident response.
Management Team	Responsible for approving and directing Security Policy during an incident response.

Another very critical aspect of Incident Response is having an established line of communications amongst all of the people listed in the matrix. With this, messages can be transmitted very quickly and efficiently. This topic will be reviewed in a future bog.

Please contact us if you have any questions!