Incident Response Concept

Kyle M. Stecki

University of Advancing Technology

To start it off, we will go into what is Incident Response, an example of the practice and how it should be handled within a business. Incident Response is a plan or approach to a situation that has happened to or within a business and it needs addressing in some manner. It can be caused by numerous problems such as an infrastructure breach or simply a mess up made by IT. There is no set way that an incident response is handled, but there are suggestions or guidelines on how certain situations should be handled. It is a plan made by the management of the company that sets the rules and regulations for the employees to mitigate the aftermath of the problem.

An example of an incident response would be where an attacker has compromised the company’s infrastructure to either steal, change or delete the data contained within the servers. A good response will have actions already in play such as backup servers that are not held on the same network that can be used to restore the servers. A good response will also have the IT quick at work figuring out where and how the attack was dealt and working on a fix to the problem, whether it be pushing out updates to workstations or changing firewall settings to provide security against further intrusions from happening. The response plan could also involve minimizing the access the employees have to the network depending on the type of attack that had occurred. On top of planning for recovery and defense, the plan could also include involving a third-party company that works solely on cyber defense to help come in and help solve the issues. As well as defending the network, the consumers should also be warned of the breach with the possibility of their information no longer being secure and how they should handle the situation with higher management sending out notices and making a public statement.

The fundamental ways of handling an incident are quite simple. The first step is preparing your network in ways that will make the situation easier to handle. This would be done with backups of the servers and data. Second is to create a team that will go to work immediately without hesitation. Generally, this will include most of your IT employees but that of course depends on the type of the attack. Third is to create an outline of how the situation should be handled and the requirement times that should be meant throughout the situation. This will give the employees an easy to follow steps on how to handle the situation. Fourth step is to establish the strategy that will be used for recovery of the infrastructure. This is the plan on how the recovery stage will be handled for the different systems, devices, and data. The fifth step would be to practice the steps with the entire team, running a simulation of what could happen and how to handle the different steps and recovery options. The sixth and final step is the debriefing of the situation. This is how to handle the reports that should be made covering the incident and how the public is addressed in a timely and appropriate manner.



References

Lily Teplow. (July 25, 2018). “6 Steps to Build an Incident Response Plan”. Retrieved from: <https://www.webroot.com/blog/2018/07/25/6-steps-to-build-an-incident-response-plan/>

Margaret Rouse. (June 2019). “incident response”. Retrieved from: <https://searchsecurity.techtarget.com/definition/incident-response>