Week 6 Case Study -

Incident Response Policy

Anthony Meunier

DeVry University

SEC 280

Week 6 Case Study – Incident Response Policy

With the amount of threats constantly evolving and growing in number, it is vital for any organization to have proper security measures in place to help protect their network and systems. The reality of network security, however, is that not all attacks are completely preventable. In the case of Gem Infosys, firewall, multiple separated servers and even an authentication server were not enough to prevent a crippling two day shutdown caused by malicious malware attacks. It is for this reason alone that it is imperative for Gem Infosys, and any organization with important data, to have an incident response policy in plan so that operations are less effected in the case of attacks or disruptions in service.

Some key points in an all-around incident response policy include areas such as disaster recovery and business continuity. By developing an incident response team and defining guidelines for them to follow and enact in the case of an incident, the recovery time can be vastly increased. A policy and its entire underlying framework should also emphasize and practice some concepts as well in order for it to be truly useful and dependable. Some of these concepts in creating a useful policy include being: succinct, understandable, practicable, cooperative, and dynamic. Let’s explore how a policy is developed.

A good incident policy can serve as an informed guide for an organization’s information activities. It sets the groundwork that shows how an organization values its information security and also displays that the organization has properly configured itself to meet needs in order to protect information security. If there are guidelines for people to follow, it becomes a much easier and more streamlined way for the organization to be protected through those involved displaying decisive and correct responses as designated in the policy. An incident response policy and included disaster recovery plan detail responsive action when passive controls fail, such as what happened with the Malware attack on Gem Infosys.

Process flow helps explain and illustrate the actions to take when they are needed. Process flow can be thought of not only as the action required, but also as the heart of what makes incident response function. The flow obviously begins when an incident occurs; from that point we go down the hierarchy of the flow to initial logging of the incident which then helps determine the urgency required. Once the urgency is determined (as low, medium, or high) the proper channels can then be followed which all detail the level of action required. If it’s a low priority response, you may need to work with relevant departments to remedy the incident and maybe consult with public relations to see if it should be made public knowledge. In a high priority response, you may add additional steps such as contacting law enforcement and so on.

As always, for any type of system security there needs to be a backup plan in place before it is too late. This falls under disaster recovery, and can include areas such as remote backup locations and offsite equipment. In addition, a strong commitment from management to provide the tools needed goes a long way in influencing everyone in the organization to feel passionate about and adhere to the policies in the best ways possible. The fact that information systems have become part and parcel to most organizations’ business processes is the most influencing reason for those organizations to have a detailed and practical incident response policy in place; practicing and protecting information security helps ensure that a business remains successful in today’s day and age.

References

Mullins, M. (2005, July 5). Create an incident response policy. Retrieved December 3, 2014, from <http://www.techrepublic.com/article/create-an-incident-response-policy/>

Wright, T. (2001, September 18). How to Design a Useful Incident Response Policy. Retrieved December 3, 2014, from <http://www.symantec.com/connect/articles/how-design-useful-incident-response-policy>