Example of research paper on policies to mitigate advanced persistent threats

Business, Company

Advanced Persistent Threats or most commonly known as APTs have been the buzzword around companies since Google announced having been a victim of it in 2010. These types of crimes are usually focused on businesses and political targets. They are referred to as advanced because they utilizes computers and advanced technology when attacking, persistent because background study and careful monitoring and analysis is done before initiating the attack and considered as threat due to the fact that these attacks involved human interventions usually by experts (Damballa, 2012). Companies are having the biggest risks of being attack by APTs because their security is the most vulnerable. APTs can breech a company's " secured network" either through internet or physical malwares or external exploitation. External exploitation can either be from an insider or from penetrations to the company's network connections outside (Damballa, 2012).

Threats from an insider have been one of the most destructive to companies. Several policies especially on ways of mitigating attacks of APTs have been outlined by companies. An effective policy that has helped companies reduce APTs is the separation of duties of personnel specially those personnel who are exposed to vulnerable data. Administrators for example for example should have different functions as those other privileged users. By doing this, specific users will only have access to specific data preventing them access to other vulnerable data that they could connect to data they have access to and make the attack. Access to other levels would need the approval of other privileged users . Since, APTs are caused by humans; the most effective way to mitigate the risks of APTs in a company is to be able to

control its human resources. Chances are, there are insiders who are capable of APT attacks.

Aside from this, companies must ensure that employees must be well educated and aware of these issues. Policies regarding their computer use must be outlined by the company and made them agree to take precautionary measures. Different access levels to specific data and networks must also be implemented by companies. In this way, there is control on what employees are able to access. Firewalls and virus and malware detections software must also be in place to be able to control incoming files that could be carriers of malwares (Public Safety Canada, 2011).

References

Damballa (2012, February 17). “ Advanced Persistent Threats”. Retrieved from http://www. damballa. com/knowledge/advanced-persistent-threats. php

Public Safety Canada (2011, December 02). “ Mitigation Guidelines for Advanced Persistent Threats”. Retrieved from http://www. publicsafety. gc. ca/prg/em/ccirc/2011/tr11-002-eng. aspx

“ How to combat advanced persistent threats: APT strategies to protect your organization” (2012, February 17). ComputerWeekly. com Retrieved from http://www. computerweekly. com/feature/How-to-combat-advanced-persistent-threats-APT-strategies-to-protect-your-organisation