Research paper on honeypots to implement of not to implement

Technology, Internet

That is the Question

Honeypots: To implement or not to implement, that is the question

There are several questions that a company needs to consider before implementing a honeypot. What type of data or information does it aim to protect? How many internal and external users access the network? Will remote access also be provided? If yes, would such access be given across geographical locations? . Honeypots do not store all interactions on a network but only direct interactions with them. Hence, the data set is limited but of great value. This also means that resources used for creating a honeypot will be minimal. Honeypots are very simple to create and maintain , and are highly flexible in detecting and adjusting to new tools and tactics that may be used against them. Hence, organizations with limited budgets and resources that consider themselves to be prone to external hacker attacks may implement honeypots.

However, honeypots only detects attacks that are directly aimed at them and hence, attacks of other systems will go undetected. Also, small errors in the creation of the ‘ entrapment’ may divulge to hackers that they are interacting with a honeypot . Should a hacker gain control over a honeypot, they may easily affect other systems within the organization. Finally, malicious internal users who are aware of the existence of the honeypot will be able to bypass it. Hence, organizations that are looking for comprehensive wide-spectrum and nearly foolproof defence systems may not prefer honeypots.

Works Cited

Spitzner, L. (2002). Honeypots: Tracking Hackers. Boston, MA: Addison-Wesley Pearson Education.

Spitzner, L. (2002). The Honeynet project: TRapping the Hackers. IEEE Security and Privacy , 1 (2), 15-23.

T., C., & Walsh, P. (2009). Chapter 4, Guarding Against Network Intrusions. In J. R. Vacca, Computer and information security handbook. Boston, MA: Morgan Kaufmann Publishers.