Week 04 Assignment 4-3

William Slater

CYBR 625 – Business Continuity Planning and Recovery

Bellevue University

The Pro's and Con's of Using Open Source Software to Defend an Enterprise Infrastructure

Sue Sampson, M.S. - Professor

September 23, 2012

The Pro's and Con's of Using Open Source Software to Defend an Enterprise Infrastructure

This brief paper will discuss the arguments for and against the adoption of open source software for the purpose of protecting an enterprise infrastructure. It will also list some open source tools and how these tools could be used to help an organization secure the enterprise while contributing toward the effort of overall goal of cost reductions in technology budgets.

The Case in Support of Open Source Software to Defend an Enterprise Infrastructure

Since the economic crash of 2008 and the recession that followed, organizations that have managed to survive have been required to make serious decisions about all business expenditures, especially those related to Information Technology and security. In many cases, this new reality has meant staff reductions, reduction in operating budgets, delaying or eliminating capital expenditures, and doing more with less.

One more pressure facing businesses is that the challenges related to security have dramatically increased over the past 10 to 15 years, as the prospects of data breaches and other security challenges continues to rise, the tools and services market has continue to grow (Verizon, 2012).

Fortunately, the open software movement that began under the leadership of Richard Stallman has given rise to a new model of software development and a new community of users that uses this open software. This is a community in which developers, usually connected via the Internet, have enthusiastically contributed their time, energy and talents to create software products that in most cases are virtually free (Gonzalez-Barahona, J. M., 2000).

The steady evolution and maturation of many of these open source software tools has created a whole new set of viable options, particularly in the area of providing security for the enterprise. These are some steps that an individual must follow to sell the management of an organization that open software solutions could meet the organization's security needs, while helping ensure that costs are contained:

1. Analyze and thoroughly understand the business and technical needs of the organization, particularly in the area of security so that the correct open source security tool can be selected for each identified need.
2. Provide accurate, objective information and case studies to the decision makers.
3. Ensure that the organization has the budget to evaluate the tools, and to train the staff to effectively use the tools that are selected and approved.
4. Ensure that experts can be identified and funded if a tools investigation process is approved.
5. Increase your specific open source tools knowledgebase by connecting with local user groups or those that you can connect with via the web.
6. Obtain permission for a pilot and possibly a benchmark demonstration to demonstrate the effectiveness and the viability of each of the tools.
7. Conduct a pilot or benchmark of the tools that are approved for investigation.
8. Write up the results of the tools pilot or benchmark, and present it to management.
9. Be sure to provide a cost benefit analysis report showing the savings of selecting open source security solutions over tools provided by commercial vendors (Seagren, E. 2007).

The Case against Open Source Software to Defend an Enterprise Infrastructure

These are the arguments against the use of open software security products:

1. If the software is open and supported by a group of individuals, it can often be considered inherently less safe than the commercially available, competing software products. This is because the code is "open" and worked on my individuals are not paid.
2. Individuals who support open software security products could possibly be bought off to write code that is exploitable, or that has Trojans or logic bombs.
3. The organization has no one to hold legally responsible if the open software security tool does not perform, or if it breaks down, or damages some part of the software or hardware infrastructure.
4. In a for-profit enterprise, stakeholders and shareholders may question the wisdom and the risks of making the decision to choose open source security tools for the enterprise.
5. The organization's business environment pressures and demands may require levels of technical support that will never be available for open source security tools.
6. The organization may not have a high enough level business and technology evangelist / champion to support the success adoption of open source security tools. Such an individual needs to be able to withstand the possible political attacks that could come from opponents of open source security tools.
7. There may be too much FUD associated with the adoption of open source security tools. FUD is Fear, Uncertainty, and Doubt.
8. The organization's overall culture may not support it.

Some Open Source Tools that Can Help Secure the Enterprise

The table below contains a short list of security-related open source tools that can usually be used to help secure the enterprise in a more cost effective manner than commercially available tools.

Tool	Use
Metasploit	Automated Attack Scripting and Exploit Simulator
MRTG	Multi Router Traffic Grapher (MRTG) is a tool to monitor the traffic load on network links (Seagren, E. 2007).
NESSUS	Network Vulnerability Scanner (Rogers, R., 2008).
NMAP	Port Scanner – Active and Passive (Seagren, E. 2007).
OpenPGP	Encryption of e-mail and e-mail attachments. (Lockhart, A., 2007)
OpenVPN	Encryption network traffic and enabling a secure virtual private network. (Lockhart, A., 2007)
OpenWRT	Firmware for monitoring of wireless traffic. (Lockhart, A., 2007)
SNORT	Network Intrusion Prevention System (NIPS) (Seagren, E. 2007).
Wireshark	Packet Sniffer (Seagren, E. 2007).

Table 1 – Partial List of Open Source Security-Related Tools

Conclusion

Ultimately, business decisions such as the selection of a security-related tool to protect the enterprise hinge on two major issues: Risk reduction and the total cost of ownership. This paper has attempted to present cogent arguments that support the positions of for and against the

introduction and use of open software security tools. In the long run, if an organization can accept the risks associated with using open software security tools, the benefits in terms of lower total cost of ownership may outweigh any possible perceived disadvantages, and the ability to provide increased security for lower costs may enhance the organization's ability to conduct its business operations (Seagren, E., 2007).

Personally, I believe that smart organizations will opt for a mix of tools that feature the advantages of selecting best of breed in both commercially available security tools and open source security tools. For example, a company where I worked in 2011, was a totally committed to the use of Microsoft, Cisco, and Oracle products, but when it came to the need for Honeypot technology, and vulnerability scans, they were totally committed to open source products, like the Honeypot Project and Nessus. The results of this combination of technologies helped the company meet its stated business and security objectives and the senior management supported those who had made the decisions and then implemented and maintained these solutions.

References

Bayles, A., et al. (2007). Penetration Tester's Open Source Toolkit, Volume 2. Burlington, MA: Syngress.

Calder, A. and Watkins, S. (2010). IT Governance: A Manager's Guide to Data Security and ISO27001/ISO27002, 4th edition. London, UK: Kogan Page.

Cole, E., et al. (2009). Network Security Bible, second edition. Indianapolis, IN: Wiley Publishing, Inc.

Harper, A., et al. (2011). Gray Hat Hacking: The Ethical Hacker's Handbook, third edition. New York, NY: McGraw Hill.

Lockhart, A. (2007). Network Security Hacks: Tips & Tools for Protecting Your Privacy, second edition. Sebastopol, CA: O'Reilly.

Osborne, M. (2006). How to Cheat at Managing Information Security. Rockland, MA: Syngress.

Rogers, R., et al. (2008). Nessus Network Auditing, second edition. Burlington, MA: Syngress.

Seagren, E. (2007). Secure Your Network for Free: Using NMAP, Wireshark, SNORT, NESSUS, and MRTG. Rockland, MA: Syngress.

Stallings, W. (2011). Network Security Essentials: Applications and Standards, fourth edition. Boston, MA: Prentice Hall.

Version. (2012). The 2012 Verizon Data Breach Investigations Report. Retrieved from http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf on September 17, 2012.

Whitman, M. E. and Mattord, H. J. (2007). Principles of Incident Response & Disaster Recovery. Boston, MA: Course Technology – Cengage Learning.

Gonzalez-Barahona, J. M. (2000). A brief history of open source software. An article published on the web on April 24, 2000. Retrieved from http://eu.conecta.it/paper/brief_history_open_source.html on September 23, 2012.