

Will Your Network Pass a Security Audit?

by: Michael Bruck, 02/17/2004

<http://www.securitydocs.com/library/23>

It is a well-known fact that in the Internet-connected world network perimeter vulnerabilities do exist that allow unauthorized individuals access to networks and provide the ability to disrupt business continuance. Well-prepared companies do know about many of these vulnerabilities and they correct them whenever appropriate. However, there are a large number of new, as well as older vulnerabilities that the average company is just not aware of.

If these vulnerabilities are known, companies usually, and I emphasize usually, allocate resources to them. Unfortunately, too many companies either do not have the resources to track such security-related matters or do not have the trained internal personnel to allocate towards identifying and remediating the vulnerabilities.

Obviously knowing about or being able to detect the vulnerabilities is half the battle, but not acting on the known issues for any reason is almost a guarantee to lose the battle.

An alarming fact is that many companies do not prioritize information security because it does not generate revenue for the company. However, as we have seen in the headlines and trade journals, the lack of a proper security program can and does affect the bottom line.

Some organizations are now investing larger budget dollars and resources into information security, and they are starting by assessing their present level of risk with an audit. If your company relies on the Internet and was one of vast number that missed the vulnerability used by the Code Red virus, you know how the lack of an active security program can affect the bottom line.

In addition to unknown vulnerabilities, there are many stories of technicians performing routine network maintenance and unintentionally leaving credit card database or other proprietary information open for would be hackers. Finding the vulnerabilities in your environment is vital to the success of your security program, but knowing how to prioritize and perform proper remediation is often impossible without properly trained personnel. Lets concentrate on the value of the audit process and deliverables for a moment.

Whenever we think of audits, the first thing that comes to mind is the financially related IRS visit. They are looking for holes in the integrity of income and expense reporting for individuals and companies. These audits are required because if the system, in this case the tax system, has enough vulnerabilities, then the whole system fails. The audit acts as the police to either deter the vulnerabilities or find them so they can be eventually removed. Removing vulnerabilities in your information network is just as key, but can you find them, which are important, and how do you remove them efficiently.

Much like the IRS audits, finding information network security vulnerabilities requires a trained professional. Most commonly, the security professionals trained in auditing are full time in-house employees of only the largest companies. For the majority of companies who want thorough periodic audits, this requires the use of outside security experts as the most cost-effective choice.

Outsourcing to security professionals offers many advantages over in-house testing, such as having a team of experts dedicated to current security matters, armed with proven best practices or entire methodologies, and equipped with a suite of security auditing products instead of a single commercial

tool.

Companies must also consider the value of the audits deliverables/results. Deliverables must not only detail all of the current vulnerabilities, but also prioritize what issues are important, document proven methodologies for remediating the vulnerabilities, and provide cost-effective methods to mitigate the risk.

The majority of companies cannot afford to maintain the staff and application software necessary to conduct an audit at this level. Even those companies that do have such a significant security budget often use an outsourced firm to validate their own efforts.

Some additional benefits of a professional outsourced audit are: recording an objective baseline and changes on a periodic basis, having a trusted security partner to turn to as issues arise, and the ability to meet industry requirements for objective third-party auditing. For those companies outsourcing audits as a secondary check, it also assists in justifying security budgets, by validating the current security-related expenditures.

Although it was mentioned that companies are sometimes challenged with prioritizing security matters, based on our own experience there is a trend with technology executives, to place a higher priority on network security. The newfound emphasis applies to both internal and external audits and really comes into play with those companies that have a great reliance on the Internet and business continuance.

Finding all of your vulnerabilities is increasingly difficult without a full suite of auditing tools, but remember, finding the vulnerabilities is only half the battle. In order for audit deliverables to be truly effective they have to include professional feedback on what issues are important, remediation efforts detailed and prioritized, as well as describe how all of the effort and expense will affect the level of risk.

If you feel your systems environment could pass a security audit, but haven't had one, our experience shows you might be surprised by a failing grade. If you have had an audit and the vulnerabilities were exposed, hopefully you have an action plan you are utilizing to eliminate the vulnerabilities. Once the action plans are complete, you might consider outsourcing your next audit to validate your efforts.

About the author:

Michael Bruck is the founding partner of Bruck and Associates, Inc. an 8 year old Information Security consulting firm. Mr. Bruck leads his security team with a successful 16-year background in IT management and senior engineering positions. He can be reached through the website at <http://www.bruck-inc.com> or by email: info@bruck-inc.com.