



Vulnerability Management – Waging War in the Homeland!

The very software that serves as your trusted business ally can be turned against you over night. It doesn't even matter how. What does matter is how you are going to know and how you are going to respond.

Vulnerability Management is referred to here in the context of a company's software portfolio and is a key contributor to the information risk management process. Managing the risk that software you use may be used against you is a familiar concept in the age of computer viruses like Code Red and Nimda. Both exploited software vulnerabilities that could and should have been managed to the point of elimination. The reasons cited by victims of these vulnerabilities range from ignorance to indifference. Anyone who had to clean up the mess these exploits left behind knows that ignorance is not bliss and that it is not always some other chap who gets whacked by the enemy. In this respect, one fact is irrefutable: Not knowing about a risk in no way makes that risk less great. So, why does anyone wait around for months at a time not knowing? Why does waiting around to determine a risk exists seem to have so much appeal? Why is vulnerability scanning conducted so infrequently? Why is vulnerability scanning not performed much like the regularly scheduled full system scans of anti-virus software? The answer, of course, is cost. The cost of knowing can be very high. Consultants equipped with complex tools and manual analysis techniques absorb precious monies and often produce inconsistent results of variable quality. Internal teams, consisting of IT staff already pinned down by IT issues, are packing aggressive project loads and often lack the specialized skills needed. Ultimately, the benefits of allocating resources to perform this work must be justified against the risk of not knowing the vulnerability exists, which is sometimes hard to quantify in terms convincing to the CFO. There are two ways to tackle this problem: ask for more resources to allow more frequent scans or wait for the cost of vulnerability assessments to go down and become a less important factor in the vulnerability management equation.

Fortunately, the latter has come true. The wait for low cost high quality network vulnerability assessments is over. Automation and evolution have teamed up to bring high performance vulnerability assessment services to the masses. Automated scanning services based on seasoned tools and techniques have evolved into a no-impact, high frequency intelligence agents that can be custom configured to scan as often as you like. And the evolution has done more than make auditing cheaper. These scans are now more comprehensive, more consistent and yield information of greater use to all participants on the risk management team: executives, management and IT administrators alike. Additionally, setup often takes only minutes and reporting is secure and offered via a professional, access controlled portal. The battle against high cost audits, conducted by hard to find specialists is being won. No longer can budget be the excuse for not knowing where the enemy is hiding.

The secret weapon is a "managed vulnerability service" (MVS). A MVS provider is equipped with supped-up scanning technology and a vulnerability knowledge base that can supply customized, timely intelligence hot off the front line. This red-hot

vulnerability information can be leveraged to address software vulnerability risk within the threat gestation window, the same window of time that is being used to create exploits for newly discovered vulnerabilities. Using this window to identify and address vulnerabilities will minimize the risk that hackers (both internal and external) will act against you. This MVS information can also be fed into a risk management process, supplied to IT management so release management and patch management processes can be improved or, it can be used to acquire the resources needed to address the software vulnerability swiftly.

Knowing is only half the battle. As mentioned above, once the vulnerability is discovered the challenge of deciding what to do about it emerges. And the clock is ticking. Every day that goes by is another day closer to an exploit that might be used against you.

If mature information risk management policies are not in place it is prudent to adopt a process that seems appropriate for use until formal policy does exist. Either way the risk management process will consist of Risk Analysis, Mitigation Analysis and Risk Mitigation. Risk analysis involves determining if the risk is or is not acceptable or transferable. If the risk must be mitigated then Mitigation Analysis is used to determine and evaluate the options available. Once a suitable mitigation option is selected the process of implementing the Risk Mitigation plan or plans is deployed.

A managed vulnerability service combined with a simple risk management approach is inexpensive protection from vulnerable software, the enemy of predictable, available business operations. Don't let the enemy sneak up on you. Have your own sniper rifle ready.

Denny Dean is chief operations architect of Treadstone 71. Denny can be reached at ddean@treadstone71.com