The U.S. House of Representatives Committee on Government Reform
Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census

Hearing on
Information Security – Vulnerability Management Strategies and Technology

June 2, 2004

Statement Submitted for the Record
By
Steven B. Solomon, Chief Executive Officer,
Citadel Security Software Inc.

Good afternoon Mr. Chairman and members of the subcommittee.

I want to thank you for the opportunity to appear today to discuss vulnerability management strategies and technology. Before I start, I want to applaud this committee for having the commitment and vision to help our nation drive awareness and direction to the ever growing security threats facing our critical IT infrastructure.

Introduction

Today organizations face exponential growth in the number of vulnerabilities and the speed at which attacks are being introduced. At a recent DoD Information Assurance conference it was predicted that by the year 2010 we will be faced with 400,000 new vulnerabilities per year. That equates to roughly 8,000 vulnerabilities per week or one new vulnerability every five minutes. By successfully exploiting one vulnerability organizations are exposed to potentially tens of millions of dollars in economic damage. A successful attack on our nation's critical infrastructure could result in life-threatening events, jeopardize our national security and impact our way of life.

By 2010, it is estimated that there will be half a billion users on the Internet. In an open society likes ours, with disperse and complex organizations, remote employees and open access to systems, we are targets for individuals and organizations that want to attack us. We can't let 9/11 repeat itself in cyber space.

To be prepared for this onslaught we must continue to expand the foundation that this committee has initiated. Expansion must include the need for sound vulnerability management processes, supporting technology, and the necessary legislation to ensure our nation's critical IT infrastructure is protected.

Nature of the Problem

We have seen the sophistication and speed of cyber threats mature to where existing security measures such as firewalls and anti-virus software are not enough to stop these attacks. By fixing known vulnerabilities we can proactively eliminate cyber threats,

reduce risk, and deliver a more secure IT infrastructure. Organizations must take a proactive stance and implement a full lifecycle vulnerability management capability. Success requires new processes, automated technology to support those processes, and management commitment to drive the needed change.

In the public sector FISMA is helping drive initiatives and awareness for improved cyber security. We believe a key aspect of FISMA is to ensure all agencies comply with assessing, remediating and reporting on compliance; however, interpretation has not been consistent through out all agencies resulting in inconsistent actions to address the problem. However, there are some excellent examples of organizations that are taking a proactive stance and making solid progress in this battle. For example, the VA's OCIS Director, Bruce Brody, had the vision and recognized the challenge around vulnerability management. Mr. Brody has directed an organization-wide program mandating a comprehensive vulnerability management process and implementation of supporting technologies to proactively remove vulnerabilities such as unsecured accounts, mis-configurations, unnecessary services, backdoors, and software defects. Other government agencies, such as the FAA, IRS, and Department of Defense are taking proactive steps to start addressing the need for a full life cycle vulnerability management process. The DoD's information assurance vulnerability management (IAVM) initiative is working to address the problem head on. For example, the Army Chief Information Officer's information assurance efforts are aligned with DoD and together they are working to deliver effective initiatives and workable solutions. We are seeing other key branches of the armed forces coming together to address the problem in similar fashion.

In the private sector we have seen limited progress in addressing these issues. Attacks and compromises to networks occur every day. Living in a false sense of security by occasionally applying patches, not doing proper vulnerability assessments, and treating the vulnerability management problem in a reactive mode is the result of a lack of process. For most of corporate America, the process is broken and fragmented across different groups using point tools and manual techniques. There are some industries ahead of others primarily driven by mandates to drive awareness and the need to be more proactive. For example, GLB in the financial sector, HIPPA in the health care sector and Sarbanes Oxley for public companies. However, the interpretation of these mandates and the required actions to comply are too broad resulting in ineffective results leading to continuous attacks and exposure on a daily basis.

Compounding the problem across both the public and private sector is the increased number of remote users who have the ability to connect to multiple networks resulting in compromised environments. When the remote worker returns to the enterprise network their compromised environment results in the continual introduction of malicious attacks after remediation actions have taken place.

Organizations that have implemented some form of patch management tool have a false sense of security. On average only 30% of an organization's verified vulnerabilities relate to patching, leaving their networks exposed to the remaining 70% of the problem which are more dangerous and easily exploited. These products do not leverage

independent vulnerability assessment data to drive the remediation process, provide compliance reporting, or have the ability to establish security policy and enforce a secure state. Further, these products do not address the problem of full life cycle vulnerability management and effectively become part of the problem.

Addressing the Challenge

Defining the vulnerability management process has several key elements. First, the process has to be enforceable across multiple disciplines and accountable to the highest levels of the organization. In addition, the process must be pragmatic and scalable to meet the needs of large organizations dispersed across global boundaries. Once the process is defined, necessary technologies have to be employed to automate. Without automation it is impossible to address the growing number of vulnerabilities in a timely, cost effective manner. Lastly, the appropriate legislation must be established including directives to specifically address the need for sound vulnerability management practices.

The challenge for many organizations across both the public and private sectors is funding. Corporations must better understand the exposure to and liability of cyber attacks as well as the resulting benefits of implementing the correct process and technologies in their environment. Hackers and terrorists are moving faster every day and implementation of these strategies must move in sync. We must invest now to establish a base line and protect the economic future of the corporation, its shareholders, and our national security.

A Full Lifecycle Vulnerability Management Process Defined

A full lifecycle vulnerability management process provides a proactive approach to eliminating IT vulnerabilities and ensuring they do not reoccur. The first step is to identify and categorize all IT assets. The second step is to assess the environment and identify vulnerabilities. The third step requires a thorough review of each vulnerability and assessment of its criticality. The fourth step involves defining the appropriate fix and applying the fix consistently across the enterprise. The fifth, and last step, requires the establishment of security policy which defines the secure state and the ongoing enforcement of that secure state.

Automating the Full Lifecycle Vulnerability Management Process

To successfully deliver a full lifecycle vulnerability management process, automation is a necessity. The ability for multiple security and IT operation disciplines to work together requires technology that provides an integrated platform from which to manage the process. Leveraging automation will shift organizations from a reactionary to a proactive vulnerability management capability.

Technology is available today to deliver a flexible automated vulnerability management capability. A key requirement are solutions that provide seamless integration across the assessment and remediation steps of the process. Full function remediation solutions must address all types of IT vulnerabilities and provide a mechanism to: report on progress from assessment, to mitigation, to on going compliance. In order to stream line the process, solutions must provide a comprehensive library of remediation actions to

identify and fix each vulnerability along with the ability to rapidly deploy remediation actions across the network in a consistent repeatable manner. As new vulnerabilities are discovered on a daily basis there must be a mechanism to continually deliver new intelligence and remediation actions. To mitigate the impact of remote users, solutions must provide the capability to both quarantine and remediate devices upon network connection.

The commercial software industry must be involved in providing quality solutions. Industry is cooperating and working to assure success. NIAP Common Criteria certification is an excellent step in this endeavor. Yet there is no enforcement across the public sector to purchase products that have received CC certification. Agencies are purchasing and deploying solutions that are not certified, or are in the process of applying for certification with no assurances of completing the process resulting in diminished value of the certification program. We recommend the government lead the way in requiring software solutions be certified to Common Criteria EAL3 or above before they can be procured and implemented.

To further reduce risk we must address a concern with offshore development. A major portion of the software developed today occurs offshore. We must add additional controls to insure software developed overseas is secure. Software development organizations should be required to have all overseas developed software examined for malicious capabilities embedded in the code. Industry and government must work together to develop some form of standard or review process to address this growing threat.

Mr. Chairman, a few months ago many leaders in the cyber security arena came together to form an important alliance. The Cyber Security Industry Alliance or CSIA represents the latest commitment from the cyber security industry to positively enhance information security. I am proud to say that Citadel serves on the board of CSIA.

The mission of CSIA is to enhance cyber security through public policy initiatives, public sector partnerships, corporate outreach, academic programs, alignment behind emerging industry technology standards and public education. At the heart of that mission, Mr. Chairman, is the full support for your efforts and those in the private sector to make information security a core corporate governance issue at the C and boardroom levels.

Conclusion

In conclusion Mr. Chairman, vulnerability management is a core security requirement. By successfully implementing a proactive, automated approach organizations can reduce risk and minimize their exposure to cyber threats. Industry and academia must work closely with government to drive awareness, education, and provide direction across the public and private sectors to this national security problem.