APPLICATION SECURITY ASSESSMENT

In the Beginning

Data security practitioners used to just focus on the networks. They tried to identify the points of interconnection where gateways and firewalls could prevent the bad packets from mixing with the good packets. As time went by, they tried to just detect the bad from the good because prevention became problematic. So, they turned their attentions to the systems. How can we protect the server if bad packets reach it over the network? They learned to prevent the spread of problems by making the systems immune to the wide variety of viruses, worms and other network based attacks. But, ultimately, they still failed to protect the valuable data and critical processors with whose security they'd been charged.

Missing the Forest for the Trees

The problem these practitioners face derives from the fact that they cannot know what goes on inside their systems. They cannot really know what's in the data that flows over the network cables. These elements only act as the containers and pathways for the applications that operate over them. While many of these are pre-built packages (e.g., mail servers), many others are custom built or configured. Thus, even the most conscientious network or system security wonk can not address the processing that goes on. Their techniques remain powerless against flaws and weaknesses in the software.

To understand the problem, a different skill set is needed. Rather than performing network scans or system penetration test, a firm grasp of design and implementation principles is needed. Someone must take a systematic look at each application to determine if it meets its own particular security requirements.

Assessing the Security of the Software

To meet the growing need to understand not just what's crossing the network or how systems are configured, Network & Security Technologies, Inc. (N&ST) has developed a structured methodology for analyzing the actual applications that operate over the IT infrastructure. This process looks at the processing as a whole to identify security problems that can expose data, disable operations and have many other serious consequences.

The N&ST methodology looks at all aspects of the application to identify the security requirements it has and expose problems that may exist. Some of the areas we examine include:

- **Security Policy**: Does the application have a defined and explicit security policy? Is that policy well documented? Does the policy cover all appropriate areas? How does the policy relate the application security to business impacts?
- **Network Controls**: How effective are the network security controls in enforcing the policy? Are they adequate? Can they operate in concert with other types of controls to be more effective?
- **System Controls**: What system security controls are in place on the server hosts? Do they meet policy requirements? Are they adequate? Can they enhance other types of controls in place?

...CONTINUED ON NEXT PAGE

Voice (845) 620-9500 Fax (845) 512-2093
http://www.netsectech.com

APPLICATION SECURITY ASSESSMENT

- **Client Controls**: What security controls exist on the client? Do these protect the user? Do these protect the server? Is it possible to subvert the client controls to overcome server security?
- **Authentication, Authorization and Access Control**: What is the security model used? Is it adequate? What does it say with respect to users and their permissions? Can the application handle it?
- **Application and Information**: Does the software implement a defense in depth strategy? Are important security principles, such as compartmentalization, implemented?
- **Procedures**: What security procedures have been defined and documented for by the development team? Do these cover all aspects of the application security? Logging and Reporting: What security logging and reporting does the application implement? Does it record failures? Does it record attempted compromises? Does it record successful uses to maintain accountability and audit requirements?

The Assessment Process

Network & Security Technologies consultants apply expert knowledge to the challenges of your business. The electronic marketplace is a networked marketplace. Only Network & Security Technologies can deliver the right combination of veteran network expertise with a firm grasp of the security principles to keep online commerce safe.

The security assessment is a three-phase process:

I: Gather information about technology and processes through interviews, document review, hands-on evaluation, and testing.
II: Analyze and quantify the risk posed by the vulnerabilities identified in terms of both likelihood and impact.
III: Produce a plan for reducing the risk to an acceptable residual through action able recommendations.

The output of the assessment is a report that permits the IT manager and business executive to understand the probable impact of the vulnerabilities in their technology and processes, as well as the likelihood that the vulnerability will be exploited by an attack.

Assessing the Security of the Software

Network & Security Technologies security and network experts understand that no organization is well served by costly and drawn-out evaluation processes. Resources are best used to build plans and implement changes, not to analyze. Thus, Network & Security Technologies experts focus their attention on the highest network and security risks facing your organization. The assessment is a starting point; a roadmap to get on track while spending the least money. It is the modest investment that any good manager must make to guarantee a well-run business will not face a crisis of confidence by its customers or stockholders.

Network &Security Technologies
161 North Middletown Road, Pearl River, NY. 10965

Our passion for technical excellence and commitment to our client's business success results in practical solutions to complex problems