September 2003

INFORMATION SECURITY

Network & Security Technologies

Security Starts at the Beginning

by Adam Lipson

Security should be an elemental part of the application development process. Despite this basic best practice, flaws continue to be found in software, leaving enterprises exposed to worms, hackers and internal malcontents.

Why? Organizations fail to follow the best practices of software development--spending $1 now to avoid $10 in repairs later. A few fundamental, common sense principles can greatly reduce the number of application vulnerabilities. These include:

--**Training & Awareness:** Educating software designers, programmers and engineers in basic security principles will make them more aware of good security practices and help reduce the number of vulnerabilities in their code.

--**Planning:** Include security at the beginning of the software development process. Make security an essential of any application project. Remember, security is extremely difficult to bolt on the finished product.

--**Testing:** Throughout the development lifecycle, test applications for security robustness and reliability. This is more than just vulnerability reviews, but ensuring that the code meets all security expectations. Also, develop a process for evaluating and testing commercial products and applications developed by third parties.

--**Assessing:** When an application is being deployed, assess what level of security it requires and how to best configure it. Periodically, return to test the application to make sure no new security holes have been opened.

Correcting flaws identified during software security audits is expensive and time consuming. Worse, vast resources are spent on containing and recovering from exploits. Fortunately, providing development staff with the knowledge and tools to avoid many of these pitfalls is easy and inexpensive.

Adam Lipson (adam.lipson@netsectech.com) is president and CEO of the infosecurity consultancy Network & Security Technologies (http://www.netsectech.com).