Realtime publishers

"Leading the Conversation"

The Essentials Series

IT Compliance Volume II

sponsored by

SECURE COMPUTING

by Rebecca Herold

Security Products Must Be Secure

by Rebecca Herold, CIPP, CISSP, CISA, CISM, FLMI *April 2007*

Software Vulnerabilities in the Security Products Industry

Every week, it seems there are headlines about security products containing vulnerabilities that put the organizations using them at risk. For example, consider the following examples from the March 15, 2007 issue of Virus Bulletin (available at (http://www.virusbtn.com/news/virus_news/2007/03_15.xml):

- "Several vulnerabilities have been found in McAfee's ePolicy Orchestrator management tool, which could be exploited to gain remote access to systems running the software. Patches have been made available and users are advised to ensure they are applied as soon as possible. Several versions of EPO 3, as well as ProtectionPilot, are thought to be affected."
- "Trend Micro, already hit by a string of vulnerabilities in recent weeks, has suffered another problem in its antivirus engine, which could cause a full system crash on exposure to a carefully crafted malicious file. The problem, caused by a divide-by-zero error in processing UPX compressed files, affects version 8 of the Trend engine, and while some systems may only lose service from the malware scanner, Windows users could suffer a 'Blue Screen of Death' (BSOD) crash of the whole operating system."

The vulnerabilities are not found just within antivirus software. Because of the complexities involved with networks and the rapidly increasing types of technologies deployed, no computer system that is useful can be completely secure. And likewise, no computer system security product can ever be guaranteed to be 100% secure. However, business leaders must still perform due diligence when choosing a security product to ensure that everything possible has been done by the vendor to remove all known vulnerabilities, and that the vendor will continue to diligently update their product to ensure all newly discovered security flaws are quickly and effectively removed.

It is of utmost importance to implement secure networks and applications. An ongoing barrage of electronic attacks on computer systems, along with an ever-increasing multitude of threats to end-user computers requires the use of information security products. Unfortunately, many vulnerabilities are also found within the very security products purchased to protect the enterprise.

It is common for organizations to perceive an immediate need to close a vulnerability or obtain compliance by purchasing additional security hardware or software products. Often the product purchase decision is then based upon the best-sounding sales claim, what is most readily available, suggestions from colleagues, or what best fits the budget. Often in-depth review of the security product gets overlooked. Third-party independent evaluation of the product is probably the best indicator of the product's effectiveness, but oftentimes this is not available or, when it is, the depth of review of the product is not deep enough to hit the full scope of security concerns or does not cover issues unique to your organization.

A highly trusted security system yesterday may be reduced to an untrusted security system tomorrow through many means:

- A previously undiscovered vulnerability in a specific operating system (OS) or other application is announced
- An update to the software configuration is installed with flawed code
- A lapse in security procedures within the vendor occurs due to a change in key personnel
- The vendor is acquired by another company and support for the product is either discontinued or drastically reduced

It is important to keep in mind that just because a security product used to be secure does not mean it will always be secure. Individual parts of a security architecture and a system's past performance are not always indicators of future trust performance characteristics.

Costs Associated with Vulnerable Security Products

Many threats against data and resources can exist when security products contain vulnerabilities; for example:

- Bugs in operating systems and application software can create exploitable vulnerabilities
- The software may not be robust enough to prevent errors made by end users and administrators
- Programmers may forget to remove backdoors to the software before launching into production
- Disgruntled employees may make changes that create vulnerabilities that they can then exploit

What are the problems associated with implementing a substandard or buggy security product? They can be substantial:

- Inability to access critical business processes on the network for prolonged periods
- Loss of an e-commerce Web site for hours, days, or weeks
- Damaged, lost, or stolen data
- Noncompliance with applicable laws and regulations
- Civil actions resulting from privacy breaches
- And many more…

Hardened Security Software Is Necessary to Protect Business

Organizations must ensure that the security products they implement are secure. Just as you expect that the brakes have been validated to work appropriately in your new car, and that your home security system has been tested to consistently set off the alarm when an intruder tries to break in, you must also use network and computer security products that do not have any security vulnerabilities. If you do not, the security products themselves will put your business at risk.

Before making a security product investment, be sure to confirm the product is as free of security bugs as possible. By doing so, you will protect your business by:

- Providing a baseline level of security to protect your enterprise from common and dangerous local and remote threats
- Ensuring a consistent approach to securing the systems upon which your business depends
- Significantly reducing the valuable time required to perform maintenance on security products
- Preventing embarrassment or public loss of confidence due to compromise of publicly accessible systems that resulted from vulnerable security products

Examples of Security Products that Must Be Hardened

It is critical—due to the purpose and nature of the product—that security tools and solutions are hardened as much as possible.

Commercial-Off-The-Shelf (COTS) product evaluations are conducted through the National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme (CCEVS). The NIAP is jointly managed by the National Institute of Standards and Technology (NIST) and NSA and staffed by personnel from those agencies. For more information, see http://www.nsa.gov/ia/industry/niap.cfm.

The types of security products you need to ensure have hardened security include:

- Application frameworks
- Application servers
- Antivirus software
- Automation/productivity application suites
- Database Systems
- DHCP servers
- Directory services
- DNS servers
- Firewalls
- Email servers
- Multi-functional peripherals
- Network routers
- Network switches
- Operating systems (OSs)
- Vulnerability management software
- Web browsers
- Web servers
- Wireless networks

25 Questions to Ask Security Product Vendors

NIST, with sponsorship from the Department of Homeland Security (DHS), has produced the *Security Configuration Checklists Program for IT Products: Guidance for Checklist Users and Developers* (available at http://checklists.nist.gov/docs/SP_800-70_20050526.pdf) to facilitate the development and dissemination of security configuration checklists so that organizations and individual users can better secure their IT products. This document is useful and rich in detail and insights. It not only breaks down the security issues that organizations must consider when choosing a software product but also discusses the issues vendors should be addressing when creating the products. It is a great document for your IT development and implementation team to use.

The following high-level quick-use checklist incorporates some of the NIST security hardening requirements as well as leading practices and my own experiences with helping organizations choose a hardened security product. Use it to help with your security product evaluation process and to facilitate discussion with your development and implementation teams.

1. **Are the default security settings consistent with recommended practices?** It is common for some vendors to set their security settings at the least restrictive levels instead of at the level that is most secure for the majority of organizations.
2. **Could any of the security product settings cause the product to become inoperable or unstable?** New features that have not been thoroughly tested could cause the product to fail when configured certain ways.
3. **Do certain settings reduce product functionality? If so, is this documented?** Sometimes security features have been engineered in ways that cause bandwidth or storage problems, resulting in making the product virtually non-functional within enterprise networks.
4. **Do the security settings take into account recent vulnerabilities?** Security products should be updated as soon as possible to address new exploits.
5. **Did independent third parties conduct security assessments on the security product?** Third-party security assessments are increasingly showing up in requests for proposals (RFPs) and service level agreements (SLAs) for packaged and on-demand software.

> The term *on-demand software* generally describes software delivered to the customer via a network (such as the Internet) as a service.

6. **Has the security product been independently evaluated using the Common Criteria (CC)? If so, at what evaluation assurance level (EAL)?** Under the CC, different classes of products are evaluated against the security functional and assurance requirements of "protection profiles." Protection profiles have been developed to apply to OSs, firewalls, smart cards, and other products that can be expected to meet security requirements. The CC specifies a series of EALs for evaluated products. A higher EAL certification specifies a higher level of confidence that a product's security functions will be performed correctly and effectively.

> For more information about the CC, see http://www.niap-ccevs.org/cc-scheme/.

7. **Does the security product vendor disclose all vulnerabilities that exist within the software?** Some vendors only disclose vulnerabilities after a patch is ready and posted on the same day as the disclosure, even though they knew about the vulnerability long before that.
8. **What technical guidance does the security software vendor provide about vulnerabilities, including how they could be exploited, how they are currently being exploited, and how to mitigate?** Software vendors that practice customer or public vulnerability disclosure are generally diligent about explaining their mitigation strategies.

9. **Does the security product vendor have a dedicated team to assess and respond to security vulnerabilities reported for their products?** Because most software vendors have a way to report and respond to bugs, security defects should be easily added to this process.
10. **Are reported security defects treated differently than non-security defects?** You want to make sure security defects within security products are elevated to a higher priority fix.
11. **Does the security software vendor have staff to simulate security attacks against the product prior to release?** Most vendors still lack the internal expertise to dedicate staff to security-specific testing.
12. **Does the security software vendor provide severity ratings for vulnerabilities, and how they are determined?** Some companies are good at defining and sharing their severity rating system. You must understand, however, that severity is a subjective measure, so you will need to determine for yourself how severe a vulnerability is for your environment.
13. **Is security reviewed at each phase of the software development life cycle (SDLC)?** Very few companies have incorporated security within all phases of the SDLC even though this is the most effective way to ensure security works as necessary and intended.
14. **Does the security software vendor use automated tools for security testing or code review?** The use of automated tools to test security is increasing, but be sure the engineers using it are trained; there is no value in a tool that is not used correctly.
15. **Has the security software vendor created the software to ensure ease of use? What tests were performed to accomplish this? Did they use independent test groups to validate ease of use?** Even the most technically effective security product will be diminished in value if it is difficult for your personnel to use.
16. **Does the security software vendor monitor the latest attack trends in the underground community and consider how those trends may affect their software?** Vendors that are proactive with security disclosure and severity ratings typically conduct these types of activities.
17. **What are the terms of the security software vendor support agreement? Will it ensure that all critical security defects will be fixed quickly, such as within 1 month of discovery?** Few vendors will make such a statement or commit to it contractually. However, the more customers ask for such terms, the more vendors will feel pressured to quickly address security vulnerabilities.
18. **Has the security software vendor ever released an emergency security patch?** This will help point to the responsiveness of the security vendor.
19. **What is the security software vendor's patch release strategy and what tools do they offer for patch deployment?** Many, if not most, vendors do not provide regularly scheduled releases, and few offer fully tested patches. You often do not get both timeliness of a patch and a fully tested patch. You may need to decide which is most important for your organization, timeliness or fully vetted patches.

20. **What methodologies does the security software vendor use for security testing their products?** Look for methodologies adopted from NIST or based upon frameworks and standards such as COBIT, the CC, or ISO 27001.
21. **What methods does the security software vendor use to inform customers of vulnerabilities?** Registered customers should have vulnerability information disclosed to them immediately, even before the associated patch is ready. It is also good if the vendor allows you to choose the method of disclosure, such as by email or phone. Be aware that many vendors believe that no disclosure at all is the best policy, or they choose just to notify their customers and the public only after a patch is ready.
22. **What percentage of the security software vendor software development and testing team is focused on security?** A security product vendor should have staff dedicated solely to security. Look for a vendor that has personnel doing testing for all the different aspects of software quality (functionality, reliability, performance, usability, accessibility).
23. **What training does the security software vendor development and testing team receive specific to application and systems security?** They should put all their personnel through some type of security training, and they should provide ongoing awareness. Unfortunately, many software vendors still do not provide adequate security training and awareness to their own personnel.
24. **Is the security product compatible with your legacy systems?** Organizations often purchase security products only to find upon installation that the products are incompatible with the organization's existing security software.
25. **Does the security vendor have substantiated testimonials to provide from other customers who use the product? Is contact information provided so that you can contact the other customers to ask about their experiences and satisfaction with the product?** It is good to confirm from others actually using the software that it does indeed work as promised.