



Greenbone Security Manager: Quality plus the latest standards, thanks to open innovation

For Stefan Schwarz, director of the computing center at the German Armed Forces University in Munich, it is obvious that both free software and commercial appliance solutions have their place. The particular circumstances and the job specifications will determine which solution is more advantageous. That also applies to vulnerability management solutions designed to detect weak points in a network. One of the reasons he turned to the GSM 500 Greenbone Security Manager was because the company supports the development of open-source variants.



der Bundeswehr
Universität München

The Client:
German Armed Forces University in Munich
(Universität der Bundeswehr München)

3,000 students pursue a variety of majors ranging from engineering to psychology and education. Basic research, plus applied research and development projects proceed on an international stage and in cooperation with scientific institutions, government agencies and businesses.

Founded in 1973, the Armed Forces University in Munich trains officers and officer candidates. However, an increasing number of civilian students have been enrolling here as well. The compact campus, combined with plenty of individual attention, affords the opportunity for concentrated, accelerated learning. The university maintains an extensive data network plus a variety of systems that not only need to perform, but must also provide security.

someone will forget to update his Joomla content management software or will forget to choose a password when he's creating a Web site with Typo3," says Schwarz.

Automatic recognition of everyday errors
These careless errors may appear minor, but they harbor the potential of becoming dangerous. Tracking them down manually would cost Schwarz and his team around three hours daily – a costly and inefficient undertaking. The Greenbone Security Manager 500 allows Schwarz to automate this

"OpenVAS is what led me to GSM 500 in the first place. I find it absolutely remarkable that Greenbone supports development of free software and contributes actively to the community."

As the head of the computing center, Stefan Schwarz commands a legion of clients and servers distributed across a multitude of networks and sub-networks. Security is his primary concern.

His greatest challenge though, lies in the changing environment, thanks to virtual systems but also, to the constant shift of personnel responsible for IT. Another challenge is the fact that the use of social media and Web 2.0 services is prevalent at the university. "Even if all security measures are in place, it happens time and again that

task and scan his systems for vulnerabilities at intervals of his own choosing. Analyzing scans of larger system landscapes would require still more time. "What matters for me is the ability to recognize modifications and differences. They will show me where there might be a threat. What makes the Greenbone solution so valuable is that it produces scans that are reliable, regular and thus, comparable," says Schwarz.

A two-pronged approach

In addition to the Greenbone Security Manager, Schwarz also uses open source OpenVAS software. "OpenVAS is what led me to the Greenbone Security Manager in the first place," he says. I was searching for a solution that could adapt quickly to new requirements. The large, active and responsive OpenVAS community, to which even developers contributed, was what sold me. Whatever work they do here goes into the Greenbone solution as well." Greenbone products represent the ideal combination of stability and quality. What is more, they are always up to date. They only contain new functions if they have been tested thoroughly first. They have to be stable and secure, and they have to furnish reliable information.

Greenbone supports the OpenVAS community explicitly. Dedicated users make sure that improvements and software adaptations are available in timely fashion, or they find prompt answers to unusual security inquiries. Of course, anyone can use the software to check for vulnerabilities, free of charge.



"There's really no alternative to the Greenbone solution if you want to use the vulnerability scan in a productive environment and you need to guarantee availability."

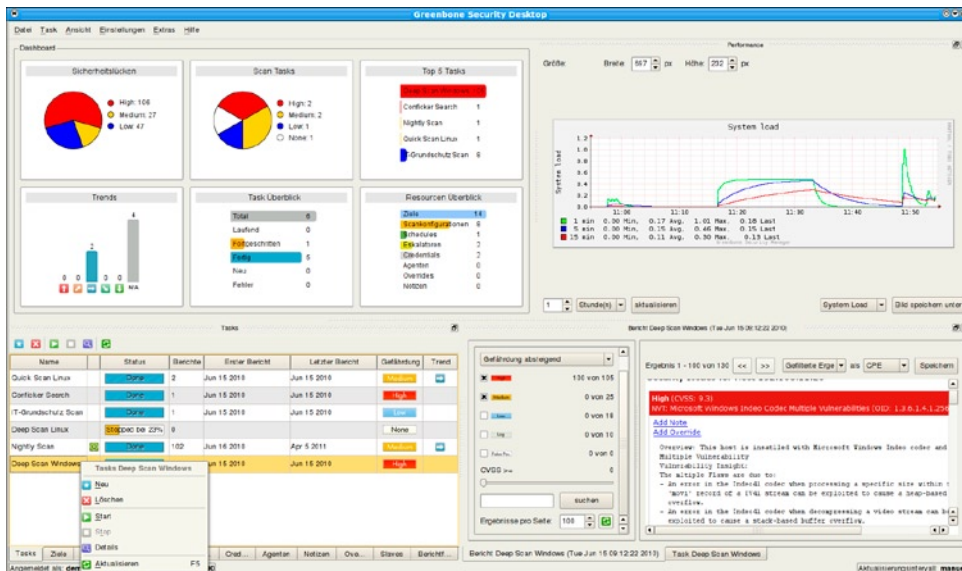
Stefan Schwarz, director of the computer center at the Armed Forces University in Munich



Priorities for the production environment

"It doesn't make much sense from a business perspective to use free software if they can have the Greenbone appliance, though," says Schwarz. "Free software is up to date and versatile but it is also prone to development errors and you need solid programming and network skills to make the best of it. Or to put it another way, you

an ongoing, but time-consuming feature as well. Open source, however, is an important system supplement for Schwarz that allows him to experiment, acquaint himself with upcoming specifications, and interact with the community. For example, he hopes that future versions will feature enhanced ability to check applications for vulnerability.



GSM 500

Areas of Application

- Medium to large IT departments
- Large branch offices
- Control of up to 10 scan sensors
- 500 - 5000 IPs

Functions

- Turnkey solution: starts up in less than 10 minutes
- Powerful operating system: Greenbone OS features; specially adapted command-line administration
- Integrated Greenbone Security Feed with more than 25,000 tests for network vulnerability and daily automatic updates
- Integrated backup, restore, snapshot and update
- Integrated Greenbone Security Assistant as the central Web interface
- No limitations on the number of target systems/IPs (the maximum number depends on the scan pattern/objectives)
- Purchase includes the right to exchange defective hardware, access to Greenbone Security Feed, feature updates and support

"What matters for me is the ability to recognize modifications and differences. They will show me where there might be a threat."

need to be your own quality manager," Schwarz cautions. "There's really no alternative to the Greenbone solution if you want to use the vulnerability scan in a productive environment and you need to guarantee availability. It gives us reliable service; there haven't been any failures. It delivers exactly what I need."

Easy operation saves time

Schwarz figures that even uninitiated users can get up to speed with the Greenbone box system within a brief time. The open source variant, on the other hand, requires experience and at least a day's work due to the constant updates. The updates are

Dedicated to openness

Aside from the benefits conferred by availability, stability and quality, Schwarz has opted for the commercial solution as a way of recognizing Greenbone's openness. "I find it absolutely remarkable that Greenbone supports development of free software and contributes actively to the community. I have seldom experienced such a dedicated, accessible and cooperative provider. I'm happy to support them by buying their solution."