Vulnerability Management with Greenbone and Nagios/Centreon: The sooner you recognize a problem, the faster you can react

“React quickly, economically and precisely” is how Jens Syckor, the head of IT security at Dresden Technical University, puts it. Recognizing a problem quickly, though, is not enough for him. Together with Greenbone, he initiated a solution for the university that integrates the Greenbone Security Manager with Nagios/Centreon monitoring software. The solution furnishes administrators all the data they need on an uncluttered dashboard without delay so that they can react quickly whenever necessary.

TECHNISCHE UNIVERSITÄT DRESDEN

The Client:
Technische Universität Dresden
The university comprises 14 faculties offering a broad range of subjects. A hotbed of research among German institutions of higher learning, it employs more than 5,000 people in state-funded positions, including 507 professors. Third-party funding provides another 3,000 jobs. The staff guarantees optimum educational opportunities for 37,000 students.

Technische Universität Dresden is one of the 11 top universities in Germany. The university stresses practical applications and interdisciplinary cooperation, and students get involved in cutting-edge research projects early on. This also makes the university an important factor for the industries that have settled in and around Dresden and in what has come to be known as Silicon Saxony. Infineon, Globalfoundries and Volkswagen are just some of the high-tech enterprises that have found a home there.

“We only authorize external Internet access to a university system once the vulnerability scan reveals that there are no problems.“

“The fact that we cooperate so closely with businesses means that we have to set very high standards for our IT as well“, explains Jens Syckor who is responsible for IT security at Technische Universität Dresden.

Automated Process for DFN-CERT
In order to detect vulnerabilities promptly, the university has long availed itself of the security bulletins issued by DFN-CERT, the computer emergency team of German research network DFN.

Originally, the university received vulnerability information via e-mail. “But it just wasn’t a professional way of doing things any more”, recounts the IT expert. “The number of potential threats has increased exponentially. We received more than 2,000 last year alone. Every time we received an e-mail, we would first have to check manually whether we were affected and then we would have to take whatever measures were necessary. We desperately needed a solution with an automated process”.

Turnkey Security
The solution of choice was the Greenbone Security Manager. “Greenbone offers two big advantages over other providers. For one thing, the company works together with DFN-CERT so that its bulletins are already part of GSM. For another, it offers the transparency we need since it is open source. That allows us to see how we are processing our sensitive data and with what”, Syckor continues.

What also tipped the scales in favor of this solution was the fact that it supports lots of different operating systems. It is easy to implement since it comes as a nearly turn-key box. Good support and daily high-quality vulnerability bulletins were critical for the university, particularly since the solution was intended to suffice for the long term.

Protecting business-critical systems
The Greenbone Security Manager GSM550 will monitor the university’s “Fort Knox” – business-critical, central systems such as its mail servers, systems for identity management, and around 200 decentralized systems used by the faculty or by projects funded by third parties. These are primarily servers with a high volume of data connected to external networks such as the Internet.

The Greenbone Security Manager also works indirectly as a quality-assurance manager for the decentralized systems. External access to the Internet is only authorized once the scan reveals that there are no poblems.

“I am completely satisfied with Greenbone and the system. The interest and feedback from our administrators has also been completely positive”

Jens Syckor, IT security officer
Technische Universität Dresden

Integration with Nagios/Centreon
“Automated vulnerability monitoring worked great right from the start. We did, however, lose valuable time transmitting the bulletins to the right places. I really wanted to shorten that time”, recollects Syckor. The university utilizes the open-source monitoring solution from Nagios/Centreon for its IT pulse check. The solution monitors whether all services are functioning at their best, and whether sufficient memory, hard-drive and processing capacity is available. An obvious step was to integrate both systems.

Tailor made by the developer
“Although there already was a Nagios plug-in from Greenbone, it did not deliver the information in the detail we wanted. A short call to Greenbone was all that was necessary and they sent a small project team to take care of it”, recalls Syckor. The rollout of the tailor-made solution ensued in less than three months’ time. Administrators can now view all the up-to-date information they need about vulnerabilities by glancing at an uncluttered dashboard. They can then act accordingly and in timely fashion. “As an open-source provider, it’s in our DNA to develop our products together with our users. We like it when we get inquiries like this because we learn from them. In the end, both sides will benefit”, says Lukas Grunwald, CTO of Greenbone.

“Thanks to open source, we can always see how we are processing our sensitive data, and with what”

Open system with room to grow
The successful system is expected to grow. It will then be possible to check internal systems as well, together with Greenbone scan sensors. “We recommend the open-source variants by Greenbone to our students for their own systems in their dormitories as well”, says Syckor with a smile.

Greenbone Security Manager

GSM 550

Areas of Application

- Medium to large IT departments
- Large branch offices
- Control of up to 12 scan sensors
- 500 - 10.000 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 30,000 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

Greenbone Networks GmbH
Neuer Graben 17,49074 Osnabrück, Germany
Telefon: +49-541-335084-0
Fax: +49-541-335084-99
Email: info@greenbone.net