Automated Vulnerability Management with Greenbone and verinice: How to manage security risks efficiently in globalized corporate IT

If you don't constantly keep an eye on things, you could easily overlook something important. That can't happen though, to the Corporate Information Security (CIS) team at cable specialist LEONI AG. Centrally controlled vulnerability management provides IT specialists in remote offices with clear directives for improving their IT security. Repeated vulnerability scans result in a self-steering process. The results speak for themselves: the amount of vulnerability in the company's worldwide system has shrunk dramatically.

The Client:
LEONI AG

Established in 1917 and headquartered in Nuremberg, Germany, the company is one of the world's largest manufacturers of wires, cables and automotive electrical systems. It employs more than 60,000 people in 32 different countries all over the world and is listed on the German MDAX stock exchange.

LEONI AG has steered a successful course. In addition to customized cable solutions, LEONI is now offering its customers complete systems featuring perfectly matched components, from the wires themselves to all the necessary connecting and fastening elements. The company has a unique value chain that harbors plenty of synergies. It starts with the finest individual wires and optical fiber, through copper and glass fiber cable, and ends with complex automotive electrical systems with built-in electronic components. Core markets include cars and trucks, manufacturing and health care, communications and infrastructure, electrical appliances, wiring and strands. Business is booming: in 2013 group sales amounted to 3.92 billion Euros.

"We increased the efficiency of our IT team all over the world in eliminating vulnerabilities. The number of vulnerabilities worldwide has dropped to a tenth of what it was when we launched the project".

Protecting a global IT infrastructure
Success stories like these could prompt prying eyes. Protecting the company's internal IT systems is a business-critical chore. The Corporate Information Security department at LEONI AG takes its mandate seriously. Back in 2011, it opted for an automated solution based on Greenbone Security Manager to counter vulnerability. The goal was to help specialists at headquarters keep the security level of the IT system in each of the 32 different countries at a uniformly high level. Christian Eschenlohr, Corporate Information Security Manager at LEONI AG, says, "Our corporate network currently comprises some 18,000 Windows systems scattered all over the globe. Today, the majority of them get scanned regularly for vulnerability - which means that we are almost there".

Recognize vulnerability before someone else does
What spoke for the Greenbone Security Manager was the fact that it could be integrated transparently into an existing infrastructure. Every step could be automated to a large degree. What's more, it helps prevent attacks and it uncovers infringements of both corporate security guidelines and of legal requirements.

Since a vulnerability report can contain hundreds of entries, LEONI chose very early on, together with Greenbone and with SerNet, to mesh the existing verinice.PRO infrastructure and the Greenbone Security Manager. They can now eliminate vulnerabilities much more efficiently.

A clear message: results
The goal was obvious: the process, from the vulnerability analysis by the Greenbone Security Manager to the issuance of directives via verinice.PRO had to be as automated as possible. The CIS team adds directives specific to LEONI to any vulnerabilities detected. The data is then imported to verinice.PRO, grouped, and transmitted to the appropriate IT specialists via e-mail.

The process takes into account how the IT specialists work, and groups the vulnerabilities accordingly. The specialists confirm when a task has been accomplished and verinice registers the fact. Confirmation can be via the verinice rich client or the verinice web front end.

Case Study Vulnerability Management
LEONI AG

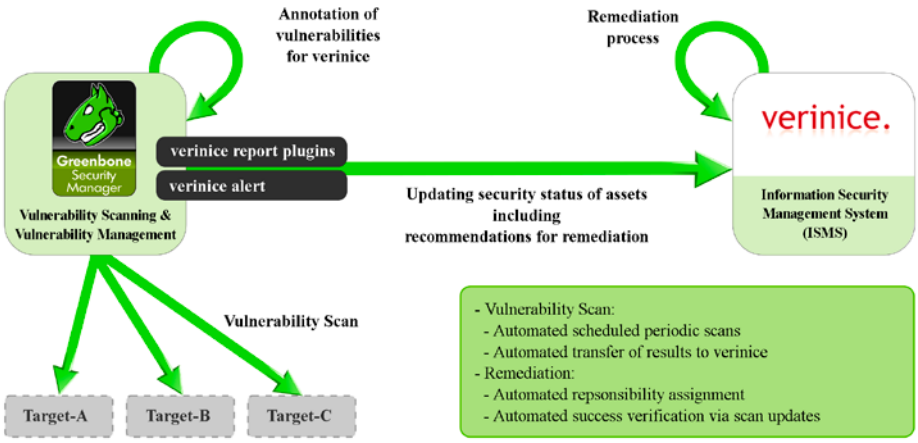
“This project enabled us to raise awareness among our IT specialists and helped us to support them in their work”.

Christian Eschenlohr
Corporate Information Security Manager LEONI AG

90 percent less vulnerabilities
Eschenlohr says: “We increased the efficiency of our IT team all over the world in eliminating vulnerabilities. The new process allows us to transmit tasks that we have checked and provided with instructions. For example, we might recommend installing a new version of a program instead of eliminating 20 vulnerabilities. Or we might recommend demanding installation of security updates only after LEONI has approved them”. The level of security has risen significantly even though CIS is spending less time on this particular aspect. Since the start of the project, the number of vulnerabilities worldwide has shrunk by ninety percent. The Greenbone solution also allows LEONI to meet VDA ISA requirements.

It’s no wonder that Eschenlohr is so enthusiastic. “Introducing the Greenbone solution has given us a real boost. Security enjoys higher priority in our company today. This project enabled us to raise awareness among our IT specialists and helped us to support them in their work”. The security expert is also pleased at how easy it is to work with Greenbone. “Everyone has learned from this project”.

Ongoing development pays off
Lukas Grunwald, CTO at Greenbone, seconds that. “With projects as big as this one, with lots of networks in different time zones, there are always going to be demands that we’ve never faced before. The effort is worth it for both sides. Customers benefit because they get a solution tailored to their needs. We benefit because the things we have learned go into our products. That means ultimately that Greenbone solutions are getting better and better”.



“Introducing the Greenbone solution has given us a real boost”.

Eschenlohr identifies still another benefit. “The big-time flexibility really impressed us because the solution can be adjusted for any location. That’s important because the situation is different from country to country. It also depends on a company‘s size. Depending on responsibility for the IT infrastructure, we generate different GSM scans. We then assemble them in verinice or we display them separately”. He adds: “Opting for Greenbone was the right move, by all means”.

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 33,000 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