tenable™ network security

OÖ.LKUF Austria

Vulnerability Analytics with New Strengths

From fast, but weekly reporting scanners to an automated, cost-saving enterprise solution: The Ober-Österreichische. Lehrer-Kranken- und Unfallfürsorge (OÖ.LKUF) institution has deployed a concept for fewer vulnerabilities and better information security using the new vulnerability management platform "SecurityCenter".

The OÖ. LKUF healthcare institution is the second largest in Austria and cares for approximately 33,000 participants. Founded 90 years ago, OÖ. LKUF covers the needs of the public school teachers in Upper Austria and is a leading healthcare institution, especially in the area of funding services. Today, OÖ.LKUF is one of the most popular health care providers in Austria.

As a statutory corporation, OÖ.LKUF is required to fulfill all duties of its board of directors, board of administration and management committee as governed by applicable laws. The organization is certified to international standards (ISO 9001:2008, NPO Label for Management Excellence) and has established stringent policies to safeguard sensitive personal data and information assets (see inset on page 2: "Privacy Policies at OÖ.LKUF") of its clients.

"IT is our backbone."

OÖ.LKUF has a security program that ensures compliance by implementing certain security measures and maintaining a security awareness program for its employees. One crucial factor of the security program is a comprehensive, reliable, and always current analysis of vulnerabilities.

"As for all modern enterprises, for us, too, IT is our backbone, which influences our business prosperity", says Dominique Höglinger, Team Leader Information Technology and CISO at OÖ.LKUF, "The fact that we have the legitimate mandate to insure teachers and that we operate with their personal health data bears additional challenges in respect to data storage and protection."

While the Nessus vulnerability scanner implemented some years ago supports our new VMware infrastructure and is still unparalleled in its detection speed and reliability, a fact that is regularly confirmed by comparisons with competing products, new challenges and complexities required capabilities found only in SecurityCenter. These included central management of multiple scanners, and advanced analytics from aggregated scan data. "The reporting," Höglinger recalls, "was performed by hand on my desk, with a lot of effort, neither comprehensive nor regularly – not what we think our security posture should be." In particular, compiling executive reports from the data was difficult, Höglinger notes. To be able to present a comprehensible report to the executive board, he had to invest hours of work copying, printing and rearranging screen shots and performing a statistical rework. All steps to create a report that was presentable to management had to be done manually.

"Once complicated, now quick and easy."

When Tenable contacted OÖ.LKUF last year and demonstrated its SecurityCenter solution on premises, Höglinger was quickly convinced of the benefits it would bring to their program. "Decisive factor for our decision was the ongoing excellent scanning results of Nessus," says Höglinger. "The scan is extremely fast, covers all vulnerabilities, even the newest, and shows appropriate mitigation options. During external tests, we experienced highly critical cases, which were, although very seldom at our organization, always detected by Nessus, but not by competing solutions."

LKUF

"SecurityCenter is a good product that met my requirements exactly. The excellent support and technical guidance provided by Tenable really convinced me. The collaboration with DigitalDefense greatly facilitated design and integration."

"SecurityCenter provides outstanding workflow management combined with the quality of the Nessus scanner, making the purchasing decision an easy one."

"It is important to me that scans complete quickly and with a high detection rate. It is also important that the results clearly describe what the vulnerability is, how it can be exploited and the remediation steps. SecurityCenter provides this on an on-going basis through a single comprehensive interface."

Mr. Höglinger

SecurityCenter combines the functionality of Nessus scanning with an enterprise-class vulnerability management platform. A great advantage of the comprehensive solution is the electronic work flow, says Höglinger. “In the case, [where] a vulnerability is detected, this allows the automatic opening of tickets and their distribution to the operative IT department. Each step can be replicated and is transparent, and most notably, the vulnerability analysis is no longer dependent on a single computer, but runs without interruption on a dedicated server.”

The permanent operation of SecurityCenter on a VMware vSphere server not only streamlines the actuality and reliability of the vulnerability analysis but also allows timed running of scans without the need of manual interference.

“What was complicated and unsatisfactory in the past runs quickly and easily today”, Höglinger summarizes. “This is the reason why in the past reports were distributed irregularly, but now are on a monthly basis, without interrupting daily operations. And if management requires a report, I can select the components that make it comprehensible and meaningful, with only a few clicks.”

Scalable Future-Proof Cost Cutting Solution

Another key benefit for OÖ.LKUF is the solution’s scalability. The company currently maintains approximately 100 workstations, mostly Windows 7 clients accompanied by some Macs. SecurityCenter is able to support much bigger infrastructures and will therefore scale with the company’s growth. This ability is enabled by the “Log Correlation Engine”, an add-on for central log analysis and event monitoring. Höglinger says: “We definitely want to incorporate this solution in the future to be able to easily view and manage error logs from different remote servers centrally.”

OÖ.LKUF expects this new approach to save even more time and money, compared to the current environment which already allows many processes to be automated. The initial investment was pretty high compared to former solutions, states Höglinger, but the license validity and automated reporting, operation, and updating will result in significant resource savings.

“The solution really pays off,” Höglinger says, content with his decision. “It virtually runs on its own and is extremely reliable. Personnel expenditures have decreased and quality has improved significantly. The product has my highest recommendation.”

Privacy Policies at OÖ.LKUF

- OÖ.LKUF uses Personally Identifiable Information (PII) only to perform its duties.
- OÖ.LKUF ensures compliance with the rights and obligations of the privacy act (Datenschutzgesetz, DSG).
- OÖ.LKUF’s employees are regularly trained in privacy and information security.
- OÖ.LKUF’s technical systems and information security measures are designed to ensure the privacy, availability and integrity of information to the extent of a reasonable economical effort.
- The effectiveness of the measures taken by OÖ.LKUF in respect to privacy and information security are continuously monitored and, if required, amended.

For More Information

Questions, purchasing, or evaluation:
Contact our EMEA Head Quarters office and we will direct your call to the appropriate local representative
sales@tenable.com or +44 (0) 203 178 4247
Twitter: @TenableSecurity
YouTube: youtube.com/tenablesecurity
Tenable Blog: blog.tenable.com
Tenable Discussions: discussions.nessus.org
www.tenable.com

tenable™
network security