Runecast
Case Study

German Hospital Saves 100s of Hours on Security Compliance

Städtisches KRANKENHAUS KIEL

Company
Kiel Municipal Hospital (Krankenhaus Kiel)

Industry
Healthcare

Location
Kiel, Germany

Employees
~2000

Summary

The Municipal Hospital in Kiel, Germany, is dedicated to providing world-class patient healthcare 24/7/365 in its region north of Hamburg. **The hospital treats over 25,000 inpatients and around 50,000 outpatients annually – and carries out around 55,000 radiological examinations each year.**

The hospital's focus centers around areas of emergency and accident care, geriatrics, surgery, hematology/oncology, urology, intensive care medicine, gynecology and obstetrics. With a women's clinic and close to 2,000 births in 2021, it managed one of the highest birth rates in the Schleswig-Holstein region.

Critical services such as initial care and aftercare for heart attack patients are handled via its cardiology clinic. All examination methods for the diagnosis of malignant organ tumors are available in the clinic for hematology and oncology. The diagnosis and treatment of patients with diseases of the esophagus, the gastrointestinal tract, the pancreas and the liver is also guaranteed in the gastroenterology/rheumatology clinic. In the field of surgery and trauma surgery, core competencies lie in general surgery and visceral surgery.

In order to provide patients with the highest standards of care, they rely on safety, quality controls and modern treatment methods. Individual departments must work closely together to guarantee that patients receive the highest level of medical care.

For holistic patient care, the hospital and its clinics work not only with internal experts and specialists, but also rely on cooperation with resident doctors and experts from the healthcare sector. Naturally, all of this is enabled by the high availability of an IT infrastructure that must be maintained in a proactive manner.

For this case study, we spoke with **Holger Lohmann, IT Systems Administrator for the hospital.**

Challenges (prior to using Runecast)

The IT team at Kiel Municipal Hospital, as a healthcare provider, is subject to increasing regulation over time. **Security and compliance were a major concern concern for their team.**

Runecast

124 City Road,
London, EC1V 2NX, UK

roi@runecast.com
www.runecast.com

"With remediation scripts alone, if I had to do all of that myself, Runecast has saved us already 100s of hours in the first few months[...] We've saved already two months of manual work in mitigating vulnerabilities."

Holger Lohmann
IT Systems Administrator
(Kiel Municipal Hospital)

They needed a way to proactively achieve and demonstrate security compliance, as regulatory bodies want to see evidence of compliance, which would have been difficult for them to provide in their previous state.

As a 'critical infrastructure' healthcare organization, the team faced the challenge of having to comply with new security regulations in the coming year. This would require an entirely different approach to monitoring the entire infrastructure for vulnerabilities and misconfigurations, and there were also Windows and Linux machines distributed throughout the hospital that would have to be covered and checked for legal requirements and vulnerabilities. Additionally, the topic of change management, documentation of such changes to the systems, and auditing were also important factors with which they needed to contend.

They were running 12 ESXi hosts, with close to 300 VMs, as well as one database cluster and a lot of Windows production machines – all of which would require detailed documentation of security measures being taken.

According to Mr. Lohmann, "Already, 50% of our time was going into security and the rest was to keep everything running. We had a reactive approach, with very limited visibility of vulnerabilities and misconfigurations."
Knowing that they would need to prove compliance with BSI IT-Grundschutz (and potentially other standards) – and lacking the confidence that they would be able to do that manually – they looked for a solution to help transform to a proactive approach.

"We needed to ensure high availability and be able to prove measures that we have taken for both vulnerability management and security compliance," said Mr. Lohmann.

Solution

Mr. Lohmann first discovered Runecast when the team were needing to manually go through VMware logs but knew that it would take far too long and needed a way to help them more easily scan the logs for any issues.

"Runecast provided exactly what we were looking for," said Mr. Lohmann, "it took us about an hour maximum to deploy the appliance, enter credentials for vCenter and run a scan."

The first Runecast scan revealed vulnerabilities, misconfigurations in their VMware security posture, and a few other bugs that needed to be addressed – including a lot of Windows OS misconfigurations that they have decided since to try to mitigate with better group policies.

"Runecast helped us to see how many systems were affected and how critical the vulnerabilities were," said Mr. Lohmann, "so in choosing our priorities we simply remediated

HIGHLIGHTS

- About 1 hour to deploy and reveal critical vulnerabilities and misconfigurations
- Critical issues now visible, easily prioritized and able to be worked on proactively
- 2 months of manual work saved in mitigating vulnerabilities
- 100s of hours saved with remediation scripts alone
- Saves the cost of them needing to find and add more team members
- Stability of mission-critical urgent-healthcare systems

the newly discovered issues from critical to medium to low."

In terms of how long it took them to mitigate the initial findings, "We were able to resolve 80% of the issues affecting our VMware security within two to three weeks. For OS, we were able to calculate that it would take a few months due to them being production machines."

They found in the Runecast platform the solution they needed for mitigating all vulnerabilities and misconfigurations in order to get their infrastructure compliant with the security regulations they would be judged against.

"We were surprised by the sheer load of information, with so many different views of the problems you're running into," said Mr. Lohmann, "but everything is in one platform and simple."

Ongoing Benefits

In terms of ongoing benefits, Mr. Lohmann stated, "Runecast helps us to harden the security of our ESXi and Windows systems – and have **everything visible in one platform, easy to handle** – so that we are able to provide the hospital staff and our patients with more reliable IT infrastructure behind the services we provide."

In the first few months after using Runecast, the team were able to clean up the major issues in their environment, and it has helped them already to gain visible control over new developments. Prior to using Runecast, they were used to dealing (reactively) with one or two minor incidents monthly and a major incident around once per quarter. After shifting some of their more reactive and time-consuming discovery tasks to a **proactive approach** with Runecast, the team has been able to focus their attention on more important projects.

"With remediation scripts alone, if I had to do all of that myself, it has **saved us already 100s of hours** in the first few months," said Mr. Lohmann. "We've saved already **two months of manual work in mitigating vulnerabilities.** The research part alone would have taken far too much of our time."

When asked which aspects of Runecast continue to surprise him and the team after working with it regularly over a longer period of time, Mr. Lohmann replied, "You get explanations of everything you need to do. Looking for all that yourself will make you crazy."

Mr. Lohmann offered the following advice to other organizations considering Runecast:

"Look how much your IT staff costs and how you can save the cost of needing to add more team members – which may not even get you to the point that Runecast does. We might have needed 1-2 more people to get close to the same work done over time, which costs even more when you factor in skills gaps and how hard it is to find security specialists."

Runecast

124 City Road,
London, EC1V 2NX, UK

roi@runecast.com
www.runecast.com