Critical digitization of the IT infrastructure of a hospital

industry

Healthcare

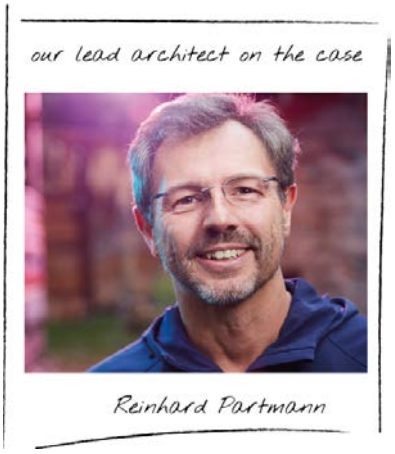
location

Germany

key challenges

- Holistic security concept for hospital IT
- Preparation of KRITIS-relevant reporting and security systems
- Management of end devices
- App management
- Ransomeware protection

Digitization in healthcare offers numerous benefits, such as more efficient treatment, better resource and staff utilization, as well as increased convenience and improved information for patients. However, more data also attracts more crime, particularly in terms of protecting patient data and ransomware.



The CTO of our customer emphasizes, "It is essential to make our IT infrastructure more resilient. Our response to ransomware cannot be to acquire ransomware pots. Especially as the hackers would also take note if we do not take sufficient measures to fend off their attacks on our systems."

Jens Hennig, comdivision's lead architect at this customer, understands the challenges: "Hospitals with over 30,000 full inpatient cases are subject to the regulations of the Critical Infrastructure Act (KRITIS). Therefore, systems for attack detection, for example, must be implemented. If a hospital receives urgently needed funding from the Hospital Future Act (KHZG), part of it is allocated to security measures."

the challenge

"The customer had already installed a variety of solutions," Hennig reports. "Most of these systems were not bad in themselves, but the associated administrative effort was immense." For this reason, the customer turned to comdivision to obtain comprehensive reports on end-device security as well as access and app security.

One of the challenges was securing device management for mobile phones, tablets, and notebooks used by employees, nursing staff, and doctors. The same applied to devices that could be used by patients. "The hospital offered

young patients the opportunity to use tablet computers for entertainment," explains Jens Hennig. "This essentially invited external access into their network, and we had to ensure that these devices did not pose a threat."

the solution

To standardize the numerous individual solutions, a new solution is being developed. "Our solution approach is based on four pillars," explains Hennig. "Device management, access (identity), app access, and antivirus/EDR threat prevention. These pillars already cover a large part of the comprehensive zero-trust architecture without completely replacing everything that already exists," says Reinhard Partmann with a wink.

At the heart of Zero Trust is an access model that grants users only the necessary permissions for the application used, without granting full access to the entire data center.

solution

A standardized solution with VMware Workspace ONE and Carbon Black has significantly reduced administrative and training overhead while improving security standards.

"It is about carefully verifying the trust relationship. First, the authenticity of the device is confirmed, followed by verifying the identity of the user and ensuring data security during transport," explains Hennig. "This process is performed for all types of applications, including cloud-based SaaS applications, on-premises software, virtual, or native applications. This process identifies the most basic permissions required for each application."

Although network virtualization is an important topic for the future, the most urgent problems had to be solved first.

Unified Endpoint Management

"Using WorkspaceONE UEM, compliance and security settings were initially set for all devices to proactively ensure that devices are always up-to-date and malfunctions are prevented through automation," explains Hennig. He adds, "We can specify that devices not only need to be patched and updated but can also automatically reinstall apps in the background, for example, to increase user acceptance and satisfaction." The hospital's CTO added, "There is an enormous training need that is difficult to meet due to the staff's workload. Simplified access control and a clear display of apps are very helpful here!"

Identity

"We migrated access control to Workspace ONE Access, which enables us to perform context-based authentication in terms of a comprehensive zero-trust architecture and implement multi-factor authentication and risk-based access," explains Hennig.

„There is an enormous training need that is difficult to meet due to the staff's workload. Simplified access control and a clear display of apps are very helpful here."

Hospital CTO

Apps/Cloud

„Our customer is progressively moving more apps from their on-premises data center to the cloud. To ensure consistent access and prevent phishing attacks, we are now utilizing Workspace ONE's Intelligent Hub to control access to cloud apps like Office 365," explains Hennig. "By doing so, we are shifting the security perimeter from the data center's firewall to the cloud, allowing for centralized management of access."

Antivirus/EDR

Through the integration of VMware Carbon Black, audit and remediation measures, also known as vulnerability management, can be implemented. Hennig describes, "with Carbon Black in the context of Workspace ONE, we harden devices to reduce the attack surface and make them less susceptible to attacks. Attacks that cannot be simply prevented through hardening must be detected and responded to. Data is fed into Workspace ONE Intelligence, where VMware SASE is used to individually decide who can access resources, when, and with which device."

summary

With this solution from the VMware Anywhere Workplace Suite, comdivision was able to prevent the threat landscape and ensure that this situation:

1. is standardized rather than isolated,
2. is viewed in context rather than as a threat, and
3. takes place in a comprehensive manner rather than in silos.

outlook

As mentioned, the customer plans to move on to the next phase of their all-encompassing zero-trust strategy after completing the remaining measures: network virtualization with NSX. Micro-segmentation allows for even more precise definition of who can access which virtual machine.

more details???

Would you like to learn more details about this or other comdivision projects? Contact us via email at info@comdivision.com, by phone at +49 251 703839 0, or check out additional case studies at https://www.comdivision.com/cd-solutions/software-defined-datacenter_-Case-Study-Section.