cryptas

we protect identities.

CUSTOMER STORY

HAUS DER BARMHERZIGKEIT

Es lebe das Leben.

BUSINESS CONTINUITY THROUGH CERTIFICATE LIFECYCLE MONITORING

HOW primeid DISCOVER HELPS SECURE IT OPERATIONS AT HAUS DER BARMHERZIGKEIT.

Haus der Barmherzigkeit is a group of facilities offering long-term care and quality of life to severely disabled people. A cross-functional team cares for 1.680 residents and clients in seven specialized hospitals, care homes, and daycare facilities in and near Vienna, Austria.

Haus der Barmherzigkeit has a particular focus on the quality of care. For this reason, the highest security standards apply also to the protection of the IT infrastructure and all personal and medical records processed within the organization. All employees are equipped with multi-factor authentication, and the server and network infrastructure is protected seamlessly with TLS certificates. Haus der Barmherzigkeit and CRYPTAS have been cooperating for many years to set up, maintain, and continuously improve these systems.

THE CHALLENGE

All digital certificates, both user and device certificates, are issued by a private certification authority (CA) operated by Haus der Barmherzigkeit.

The certificate lifecycle for user certificates is already continuously monitored and regularly renewed by a credential management system.

This is not possible for device certificates. However, device certificates are used for a wide variety of systems, from hypervisor consoles for virtualization servers, web servers, application servers, and database servers to the many WIFI access points in all care facilities. In many cases, device certificates are used for 2-way TLS mutual authentication of subsystems within the infrastructure.

The expiration of device certificates that are not renewed in time inevitably leads to system outages. Often, the cause of such outages is not immediately apparent. E.g., if a database server certificate expires, a connected application may fail without any indication. This may lead to prolonged outages and subsequently affect ongoing care services at facilities.

To address this business continuity risk, the lifecycle of all device certificates was previously managed manually. All certificate data was manually entered into a digital calendar so that all due dates came to the attention of the IT team, which in turn processed the renewals. This led to an error-prone and labor-intensive process. With the ever-increasing complexity of the IT landscape at Haus der Barmherzigkeit, a new and more automated process for certificate lifecycle management became inevitable.

THE SOLUTION

To completely automate certificate lifecycle monitoring at Haus der Barmherzigkeit, the CRYPTAS product primeid DISCOVER was deployed. primeid DISCOVER continuously synchronizes all certificates issued by the private CA and monitors them accordingly. Rules can be defined and applied for each certificate type and use case. For example, primeid DISCOVER can be configured to define who in the organization is notified of upcoming renewals and how far in advance. Based on these notifications, the IT team initiates certificate renewals. All newly issued certificates are registered automatically, eliminating the need for manual bookkeeping.

Market standard solutions for complete certificate lifecycle management are too complex and costly for Haus der Barmherzigkeit, not only in license fees but also in deployment efforts and daily operation, given the very specific but also limited nature of the task. primeid DISCOVER was developed precisely for such particular purposes and is easy to deploy and use.

THE RESULT

primeid DISCOVER has made IT operations at Haus der Barmherzigkeit more robust and resilient. The automation also led to a simplification and unification of system-critical processes in certificate life cycle management.

The product is very intuitive to use and saves us a lot of manual work in certificate management, says Thomas Schneider, system administrator at Haus der Barmherzigkeit.

Here, too, CRYPTAS was able to provide us with competent support from problem analysis to implementation of the solution, adds Daniel Fürdauer, Head of Information Security at Haus der Barmherzigkeit.