semperis

CASE STUDY POLIPOL

POLIPOL®

Good upholstered furniture is an investment which allows you to sit back in comfort for many years and forget your daily troubles. The Polipol organization is a furniture manufacturer whose strategy is a reflection of this: bringing customers comfort and doing all it can to keep on the safe side. The same applies to IT security. With the introduction of Semperis Active Directory Forest Recovery, Polipol ensures that access to its IT assets is guaranteed even in the event of a cyberattack.

> We have always been aware that AD is of particular importance for the continuity of the business processes. This is why we had tasked an external service provider with backing up the data, so we could access it if there was a breach."

Waldemar Stirtz
Head of IT Administration

ACTIVE DIRECTORY BACKUP AT POLIPOL

The history of Polipol reads like a modern-day rags-to-riches tale. Founded 35 years ago by four work colleagues, the organization today employs around 8,000 people, dedicated to the manufacturing and distribution of high-quality furniture. The little company has since grown into a global group, with several international subsidiaries and sales totaling some €600 million. It goes without saying that, in addition to growing production and sales, considerable efforts have gone into ensuring a fit-for-purpose IT infrastructure to support the business and production processes.

There are currently almost 100 employees working in IT to provide the functions that cover the span from production through administration to sales. This involves the use of central solutions, such as SAP, but also various other applications that need to be managed as part of the international consolidation process.

ACTIVE DIRECTORY AS A CENTRAL ASSET

Almost 90% of leading organizations worldwide use Microsoft Active Directory (AD) for the centralized management of their users, computers and assets in their networks. It guarantees the hierarchical structuring of access rights per domain, organizational unit or location, as well as per user and device. Based on the permissions assigned to them, users can log in to Active Directory, where they are authenticated and authorized to access the assets for which they have access rights. This makes Active Directory the central repository for the identity and access rights in organizational networks.

But what happens if Active Directory is not available, on account of a technical glitch or a potential attack on the infrastructure? This would inevitably lead to a failure of the entire IT system. It is this precise issue that Waldemar Stirtz, Head of IT Administration at Polipol, has been getting to grips with. He has been with Polipol for 25 years now and is responsible, along with his 35 or so colleagues, for global projects, licenses and other duties.

"We have always been aware that AD is of particular importance for the continuity of the business processes," says Mr. Sturtz: "We had therefore tasked an external service provider with backing up the data, so we could access it if there was a breach." However, the infrastructure has undergone massive change on account of the organization's geographical expansion. Domains have been added, and with them secondary domain controllers, which are meant to ensure redundancy, load distribution and fault tolerance for each new site. "The challenge was to manage so many new users, groups or objects, and the backup concept of the service provider we were then using no longer had us convinced."

ACTIVE DIRECTORY FOREST RECOVERY

Polipol set out in search of a secure solution to meet its needs and opted for a collaboration with Semperis and the use of its Active Directory Forest Recovery (ADFR) product, which guarantees rapid restoration of the entire AD structure in the shortest time, on any virtual or physical platform and regardless of the complexity of the infrastructure. "The more domains and controllers there are to be operated, the harder it is to structure the backup and recovery process. Anyone who, like us, operates around 30 domain controllers and 12 domains, will find several hundred pages of documentation from Microsoft Support on the topic of backup, but ultimately no practical solution," Mr. Stirtz goes on to say.

In practice, what this involves at Polipol is securing the operational continuity of around 2200 users in some 1000 groups, as well as considerably more objects, including the necessary access control concepts. This includes, as a minimum, the daily backup of data and, if necessary, restoration within the shortest possible time. This cannot be achieved with standard tools, and requires a specialized solution that is easy to implement and operate, and yet which provides the necessary functionality.

Active Directory Forest Recovery (ADFR) from Semperis is one such specialized solution for the automated recovery of Active Directory in the wake of cyber disasters. By fully automating the recovery process, ADFR significantly reduces downtime and minimizes the risk of reinfection by malware by restoring the AD on newly installed target systems to a known secure state without reinstalling the malware on the operating systems of the affected source systems.

An outstanding feature of ADFR is its ability to automate the entire forest recovery process in just a few steps, leading to rapid, clean and uncomplicated data recovery. This approach can shorten AD recovery times by up to 90%. ADFR also guarantees the creation of a replica of the AD production environment, simplifying disaster recovery planning.
By uncoupling the AD from the underlying operating system, organizations can significantly reduce the threat of downtimes.

FAST AND EASY IMPLEMENTATION

The decision to opt for the solution was quickly taken following a detailed discussion with the experts from Semperis. And the installation of the solution was just as expeditious. "All we had to do was complete a few tasks," Mr. Stirtz recalls. "We filled out a questionnaire, and Semperis designed our solution on this basis. We then managed to set up and configure the servers ourselves in less than two hours."

Indeed, the entire implementation of the backup is now in the hands of Mr. Stirtz's team. The data is also stored securely in their own data center, with the idea of taking on additional cloud storage currently being discussed.

Through the introduction of Active Directory Forest Recovery, Polipol has been able to address four key aspects which, without the software solution, would have led to restrictions on use and time-consuming manual tasks. The automatic recovery of several forest-wide structures reduces possible downtimes now to a minimum. ADFR also prevents reintroduction of malware by ensuring that only the critical Active Directory data is backed up, without the other files of the infected operating system of the AD servers (domain controllers). Recovery can take place on any virtual or physical hardware, mainly on newly installed systems, and, what is more, the forensic analysis of AD attacks is significantly accelerated, so that any remaining vulnerabilities can be quickly identified and eliminated.

Semperis ADFR uses specific mechanisms for the selection and compression of the data to be stored, thereby reducing storage needs and increasing the efficiency of the data protection. The optional encryption ensures that sensitive AD backup data is protected both during transfer and when in storage. These mechanisms enable rapid restores following cyberattacks. Executable files that may still be located in the SYSVOL folder—where the files for Group Policy and login scripts are stored—are placed in quarantine after being restored, thereby guarding against fresh infection from malware.

"Compared to the previous solution we had in place, Semperis Active Directory Forest Recovery allows us to react more flexibly to changes, and to perform backups more frequently and, above all, free from malware," says Mr. Stirtz, in summarizing the goals achieved. "It takes precisely six clicks to be able to return to work after a potential incident, and we don't have to keep starting again from scratch." After all, it would take several weeks to recreate the directory manually.