semperis

CASE STUDY POLIPOL

POLIPOL®

A good piece of upholstered furniture is an investment that provides years of comfortable relaxation and a place to forget the stresses of daily life. Polipol, a maker of classic, elegant furniture, aims to provide customers with that carefree comfort. They take the same approach to IT security. By implementing Semperis Active Directory Forest Recovery, Polipol guarantees access to its IT resources even in the event of a cyberattack.

> We were always aware that AD is of particular importance for the continuity of business processes. For that reason, we had commissioned an external service provider to back up the data so that we could access it in the event of a compromise."

Waldemar Stirtz
Head of IT Administration, Polipol

ACTIVE DIRECTORY BACKUP AND RECOVERY AT POLIPOL

The history of Polipol reads like a modern self-made fairy tale: Founded 35 years ago with four employees, the company now employs around 8,000 people dedicated to the production and distribution of high-quality furniture. From a small firm, it has grown into a globally operating group with several international subsidiaries generating a turnover of almost €600 million. In addition to setting up production and sales, significant effort was required to develop the IT infrastructure necessary to support the business and production processes.

Currently, nearly 100 employees work in IT to provide functions ranging from production and administration to sales. Central solutions such as SAP are used, as well as various other applications that need to be managed as part of the international consolidation process.

ACTIVE DIRECTORY AS A CENTRAL RESOURCE

Nearly 90 percent of the world's leading enterprises use Microsoft Active Directory (AD) to centrally manage users, computers, and resources across their networks. AD enables the hierarchical structure of access permissions by domain, organizational unit or location, users, and devices. Based on their assigned permissions, participants can log in to Active Directory, where they are authenticated and authorized to access resources.

Thus, AD serves as the central authority for identities and access rights in corporate networks. But what happens if Active Directory is not available because of a technical glitch or an attack on the infrastructure? A complete IT outage.

Waldemar Stirtz, Head of IT Administration at Polipol, had dealt with this very question. He has been with Polipol for 25 years and, with his approximately 35 employees, is responsible for IT security, global projects, licenses, and other tasks.

"We were always aware that AD is of particular importance for the continuity of business processes," explains Stirtz. "For that reason, we had commissioned an external service provider to back up the data so that we could access it in the event of a compromise." However, the infrastructure had changed significantly as a result of geographic expansion. New domains were added, along with secondary domain controllers, which intended to ensure redundancy, load balancing, and fault tolerance at each new location.

"We simply had to manage many new users, groups, and objects, and the backup concept of our previous service provider no longer seemed adequate."

ACTIVE DIRECTORY FOREST RECOVERY

Polipol sought a more secure solution and decided to work with Semperis and implement their Active Directory Forest Recovery (ADFR), which ensures a rapid recovery of the entire AD forest—on any virtual or physical platform and regardless of infrastructure complexity.

"The more domains and controllers you operate, the more difficult the backup and recovery process becomes. If, like us, you operate around 30 domain controllers and 12 domains, you'll find hundreds of pages of backup documentation from Microsoft Support, but ultimately no practical solution," explains Stirtz.

In practice, Polipol's challenge is about ensuring the continuity of around 2,200 users across more than 1,000 groups and significantly more objects, including the necessary authorization concepts. Managing the environment requires at least daily backups and, if necessary, rapid data recovery. Standard tools can't meet their needs; rather, they require a specialized solution that is easy to implement and operate and still provides the necessary functionality.

ADFR from Semperis is a specialized solution for the automated recovery of Active Directory after cyber disasters. By fully automating the recovery process, ADFR significantly reduces downtime and minimizes the risk of malware reinfection by restoring AD to a known safe state on freshly installed target systems, without reintroducing the malware to the operating system of the affected source systems.

A standout feature of ADFR is its ability to automate the entire forest recovery process in just a few steps, resulting in a fast, clean, and straightforward recovery. This approach can reduce AD recovery time by up to 90 percent. In addition, ADFR enables you to set up a replica of the AD production environment, simplifying disaster recovery planning. By decoupling AD from the underlying operating system, organizations can significantly reduce potential downtime.

QUICK AND EASY IMPLEMENTATION

The decision to use the solution was made quickly after a detailed discussion with Semperis experts. And the installation was just as fast. "This only required us to perform a few tasks," Stirtz recalls. "We filled out a questionnaire, on which Semperis based a design. We then prepared and configured the servers ourselves within two hours."

In fact, the entire backup process is now in the hands of the Stirtz team. The data is also stored securely in the company's own data center, although the idea of additional cloud storage is currently being discussed.

With the introduction of Active Directory Forest Recovery, Polipol has addressed four key issues that, without the Semperis solution, would have led to potential disruptions and time-consuming manual mitigation. Automatic recovery of multiple forests now reduces potential downtime to a minimum; ADFR also avoids the reintroduction of malware by backing up only the critical AD data, excluding infected files on the AD servers (domain controllers). Recovery can be performed on any virtual or physical hardware, usually freshly installed. And forensic analysis of AD attacks is significantly accelerated, enabling rapid detection and elimination of any remaining vulnerabilities.

Semperis ADFR uses specific mechanisms to select and compress the data to be stored, reducing storage requirements and increasing backup efficiency. Optional encryption ensures that sensitive AD backup data is protected both during transmission and in storage. These mechanisms enable rapid recovery after cyberattacks. Executable files that may still be in the SYSVOL folder—where the files for Group Policy and login scripts are located—are quarantined during recovery, which prevents malware reinfection.

"Compared to the solution we used previously, Semperis Active Directory Service Recovery enables us to react more flexibly to changes, to carry out backups more frequently and, above all, free of malware," says Stirtz, summarizing the goals achieved. Previously, it would have taken several weeks to manually recreate the directory.

Now? "It takes exactly six clicks to get back to work after a potential incident, and we don't have to start all over again."

ABOUT SEMPERIS

For security teams charged with defending hybrid and multi-cloud environments, Semperis ensures the integrity and availability of critical enterprise directory services at every step in the cyber kill chain and cuts recovery time by 90%. Purpose-built for securing hybrid identity environments—including Active Directory, Entra ID, and Okta—Semperis' patented technology protects over 100 million identities from cyberattacks, data breaches and operational errors. The world's leading organizations trust Semperis to spot directory vulnerabilities, intercept cyberattacks in progress and quickly recover from ransomware and other data integrity emergencies. Semperis is headquartered in Hoboken, New Jersey, and operates internationally, with its research and development team distributed throughout the United States, Canada and Israel.

Semperis hosts the award-winning Hybrid Identity Protection conference and podcast series (www.hipconf.com) and built the community hybrid Active Directory cyber defender tools, Purple Knight (www.semperis.com/purple-knight/) and Forest Druid (www.semperis.com/forest-druid/). The company has received the highest level of industry accolades, recently named to Inc. Magazine's list of best workplaces for 2024 and ranked the fastest-growing cybersecurity company in America by the Financial Times. Semperis is a Microsoft Enterprise Cloud Alliance and Co-Sell partner and is a member of the Microsoft Intelligent Security Association (MISA).

semperis