semperis

CASE STUDY POLIPOL

POLIPOL®

Ein gutes Polstermöbel ist eine Investition, die dazu dient, sich über viele Jahre bequem zurückzulegen und die täglichen Sorgen zu vergessen. Das Unternehmen Polipol ist ein Hersteller von Möbeln, der genau diese Strategie verfolgt: Dem Kunden Bequemlichkeit zu verschaffen und dabei alles zu unternehmen, um auf der sicheren Seite zu sein. Das bezieht sich auch auf die IT-Security. Mit der Einführung von Semperis Active Directory Forest Recovery stellt Polipol sicher, dass der Zugriff auf IT-Ressourcen auch im Falle einer Cyber-Attacke gewährleistet ist.

> Es war uns immer bewusst, dass das AD von besonderer Bedeutung für die Kontinuität der Unternehmensprozesse ist. Wir hatten deshalb eigens einen externen Dienstleister mit dem Backup der Daten beauftragt, um im Falle einer Kompromittierung darauf zurückgreifen zu können."

Waldemar Stirtz
Head of IT Administration

ACTIVE DIRECTORY-BACKUP BEI POLIPOL

Die Geschichte von Polipol liest sich wie ein modernes Self-Made-Märchen: Vor 35 Jahren mit vier Mitarbeitern gegründet, beschäftigt das Unternehmen nun rund 8.000 Menschen, die sich der Herstellung und dem Vertrieb von qualitativ hochwertigen Möbeln widmen. Aus der kleinen Firma wurde eine weltweit agierende Gruppe, die inzwischen mit mehreren internationalen Tochterunternehmen einen Umsatz von fast 600 Millionen Euro erzielt. Es versteht sich von selbst, dass neben dem Aufbau von Produktion und Vertrieb erhebliche Anstrengungen hinsichtlich der IT-Infrastruktur erforderlich waren, um die betriebswirtschaftlichen und produktiven Prozesse zu begleiten.

Insgesamt arbeiten derzeit fast 100 Mitarbeiter in der IT, um die Funktionen von der Produktion über die Verwaltung bis hin zum Verkauf bereitzustellen. Zum Einsatz kommen zentrale Lösungen wie SAP, aber auch diverse andere Anwendungen, die es im Zuge der internationalen Konsolidierung zu betreuen gilt.

ACTIVE DIRECTORY ALS ZENTRALE RESSOURCE

Fast 90 Prozent der führenden Unternehmen weltweit setzen das Microsoft Active Directory (AD) für die zentrale Verwaltung ihrer Benutzer, Computer und Ressourcen in ihren Netzwerken ein. Es gewährleistet die hierarchische Strukturierung der Zugriffsberechtigungen nach Domänen, Organisationseinheiten oder Standorten sowie nach Benutzern und Geräten. Aufgrund der ihnen zugewiesenen Berechtigungen können sich Nutzer beim Active Directory anmelden und werden dort authentifiziert und autorisiert, um Zugriff auf die jeweils berechtigten Ressourcen zu erhalten. Damit bildet das Active Directory die zentrale Instanz für die Identitäten und Zugriffsrechte in Unternehmensnetzwerken.

Aber was passiert, wenn das Active Directory nicht bereitsteht, infolge einer technischen Panne oder eines nicht auszuschließenden Angriffes auf die Infrastruktur? Das würde zwangsläufig zu einem Ausfall der gesamten IT führen. Mit eben dieser Frage hatte sich Waldemar Stirtz, Leiter der IT-Administrationsabteilung bei Polipol, beschäftigt. Er begleitet Polipol seit 25 Jahren und ist mit seinen rund 35 Mitarbeitern für die IT-Security, globale Projekte, Lizenzen und andere Aufgaben verantwortlich.

„Es war uns immer bewusst, dass das AD von besonderer Bedeutung für die Kontinuität der Unternehmensprozesse ist", erklärt Stirtz, „Wir hatten deshalb eigens einen externen Dienstleister mit dem Backup der Daten beauftragt, um im Falle einer Kompromittierung darauf zurückgreifen zu können." Allerdings hat sich die Infrastruktur infolge der geografischen Expansion massiv verändert. Domains waren hinzugekommen und damit auch Secondary-Domain-Controller, die an jedem neuen Standort Redundanz, Lastverteilung und Ausfallsicherheit sicherstellen sollen. „Es galt einfach, viele neue User, Gruppen oder Objekte zu verwalten, und das Backup-Konzept des damaligen Dienstleisters schien uns am Ende nicht mehr schlüssig."

ACTIVE DIRECTORY FOREST RECOVERY

Polipol begab sich auf die Suche nach einer entsprechend sicheren Lösung und entschied sich für die Zusammenarbeit mit Semperis und den Einsatz ihres Produktes Active Directory Forest Recovery (ADFR), welches eine schnelle Wiederherstellung der AD-Gesamtstruktur innerhalb kürzester Zeit garantiert – auf jeder virtuellen oder physischen Plattform und unabhängig von der Komplexität der Infrastruktur. „Je mehr Domains und Controller betrieben werden, desto schwieriger gestaltet sich der Backup- und Wiederherstellungsprozess. Wer wie wir rund 30 Domain-Controller und 12 Domains betreibt, findet beim Microsoft-Support zwar einige Hundert Seiten Dokumentation zum Thema Backup, am Ende aber keine praktische Lösung", erläutert Stirtz.

Tatsächlich geht es in der Praxis bei Polipol um die Sicherstellung der Kontinuität von rund 2.200 Usern in gut 1.000 Gruppen und noch deutlich mehr Objekten inklusive der erforderlichen Berechtigungskonzepte. Und dazu gehören zumindest eine tagesaktuelle Sicherung der Daten und im Bedarfsfall eine Wiederherstellung innerhalb kürzester Frist. Das ist mit Bordmittel nicht zu erreichen – vielmehr bedarf es einer spezialisierten Lösung, die leicht zu implementieren und zu bedienen ist ,und trotzdem die erforderliche Funktionalität mitbringt.

Active Directory Forest Recovery (ADFR) von Semperis ist eine dieserart spezialisierte Lösung zur automatisierten Wiederherstellung von Active Directory nach Cyber-Katastrophen. Durch die vollständige Automatisierung des Wiederherstellungsprozesses reduziert ADFR Ausfallzeiten erheblich und minimiert das Risiko einer erneuten Malware-Infektion, indem es das AD auf frisch installierten Zielsystemen mit einem bekannten sicheren Zustand wiederherstellt, ohne die Malware im Betriebssystem der betroffenen Quellsysteme dabei wieder einzuspielen.

Ein herausragendes Merkmal von ADFR ist die Fähigkeit, den gesamten Forest-Wiederherstellungsprozess mit nur wenigen Schritten zu automatisieren, was zu einer schnellen, sauberen und unkomplizierten Wiederherstellung führt. Dieser Ansatz kann die Wiederherstellungszeit von AD um bis zu 90 % verkürzen. Zusätzlich gewährleistet ADFR die Einrichtung einer Replik der AD-Produktionsumgebung, was die Planung der Notfallwiederherstellung vereinfacht. Durch die Entkopplung des AD vom zugrunde liegenden Betriebssystem können Unternehmen drohende Ausfallzeiten maßgeblich reduzieren.

SCHNELLE UND EINFACHE IMPLEMENTIERUNG

Die Entscheidung für den Einsatz der Lösung war nach einem ausführlichen Gespräch mit den Semperis-Experten schnell getroffen. Und ebenso schnell erfolgte die Installation. „Von uns erforderte dies lediglich die Erfüllung weniger Aufgaben", erinnert sich Stirtz. „Wir haben einen Questionnaire ausgefüllt, auf dessen Basis von Semperis ein Design ausgearbeitet wurde. Die Vorbereitung der Server und deren Konfiguration haben wir anschließend innerhalb von zwei Stunden selbst bewerkstelligt."

Tatsächlich liegt die gesamte Durchführung des Backups nun in der Hand des Teams von Stirtz. Auch die Daten werden entsprechend geschützt im eigenen Rechenzentrum gespeichert, wobei die Idee einer zusätzlichen Cloud-Speicherung derzeit diskutiert wird.

Mit der Einführung von Active Directory Forest Recovery hat Polipol insbesondere vier Kernpunkte adressiert, die ohne die Software-Lösung zu potenziellen Nutzungsbeeinträchtigungen und zeitraubenden manuellen Tätigkeiten geführt hätten. Die automatische Wiederherstellung mehrerer Gesamtstrukturen reduziert mögliche Ausfallzeiten nun auf ein Minimum; ADFR vermeidet zudem die erneute Einschleppung von Malware, indem schon beim Backup nur die kritischen Daten des Active Directory ohne die restlichen Dateien des befallenen Betriebssystems der AD-Server (Domain Controller) gesichert werden. Die Wiederherstellung kann auf jeder beliebigen, meist frisch installierten virtuellen oder physischen Hardware erfolgen, und außerdem wird die forensische Analyse von AD-Angriffen maßgeblich beschleunigt, sodass noch bestehende Einfallstore schnell aufgefunden und beseitigt werden können.

Semperis ADFR nutzt spezifische Mechanismen zur Selektion und Komprimierung der zu speichernden Daten, wobei der Speicherbedarf reduziert und die Effizienz der Datensicherung erhöht wird. Die optionale Verschlüsselung stellt sicher, dass die sensiblen AD-Backup-Daten sowohl während der Übertragung als auch in gespeicherter Form geschützt sind. Diese Mechanismen ermöglichen eine schnelle Wiederherstellung nach Cyberangriffen. Ausführbare Dateien, die sich gegebenenfalls noch im SYSVOL-Ordner befinden, also dort, wo die Dateien für Gruppenrichtlinien und Login-Skripte liegen, werden bei der Wiederherstellung in Quarantäne gesetzt, wodurch eine Neuinfektion durch Malware ausgeschlossen ist.

„Im Vergleich zu der zuvor eingesetzten Lösung gewährleistet es uns Semperis Active Directory Forest Recovery, flexibler auf Veränderungen zu reagieren, und das Backup häufiger und vor allem frei von Malware durchzuführen", fasst Stirtz die erreichten Ziele zusammen. „Es braucht genau sechs Klicks, um nach einem potenziellen Vorfall wieder arbeitsfähig zu sein, und wir müssen nicht immer wieder von vorne beginnen." Schließlich würde es einige Wochen dauern, um das Verzeichnis manuell neu anzulegen.

ÜBER SEMPERIS

Semperis hilft Teams, die mit dem Schutz hybrider und Multi-Cloud-Umgebungen betraut sind, die Integrität und Verfügbarkeit der kritischen Verzeichnisdienste zu sichern. Dabei werden alle Phasen der Angriffskette abgesichert und die erforderliche Zeit für Recovery um 90% reduziert. Die patentierte Technologie von Semperis, welche speziell für den Schutz hybrider Identitätslandschaften einschließlich Active Directory, Entra ID und Okta entwickelt wurde, schützt über 100 Millionen Identitäten vor Cyber-Angriffen, Datenlecks und administrativen Fehlern. Führende Unternehmen weltweit vertrauen auf Semperis beim Aufdecken von Schwachstellen in Verzeichnisdiensten, Erkennen von Bedrohungen in Echtzeit sowie beim schnellen Wiederherstellen nach einem Ransomware-Angriff oder anderen schwerwiegenden Vorkommnissen. Semperis hat seinen Hauptsitz in Hoboken, New Jersey, und ist international tätig. Das Forschungs- und Entwicklungsteam ist über die Vereinigten Staaten, Kanada und Israel verteilt.

Semperis veranstaltet die preisgekrönte „Hybrid Identity Protection"-Konferenz und produziert die dazugehörige Podcast-Reihe (www.hipconf.com). Die Firma stellt der Cyberdefense-Community die beliebten Analysewerkzeuge „Purple Knight" (www.purple-knight.com) and „Forest Druid" zur Verfügung. Semperis wurde durch die Fachpresse mehrfach auf höchstem Niveau ausgezeichnet und sicherte sich 2024 den Platz auf der Liste der besten US-Arbeitgeber des „Inc. Magazine". Laut „Financial Times" ist Semperis das am schnellsten wachsende Cybersecurity-Unternehmen in Amerika. Semperis ist Microsoft Enterprise Cloud Alliance-Partner und Microsoft Co-Sell-Partner sowie Mitglied der „Microsoft Intelligent Security Association" (MISA).

semperis