Access Management bei Gedore

Rechtevergabe von Anwender zu Anwender

Die 1919 gegründete Gedore Werkzeugfabrik ist heute als Hersteller von Premiumwerkzeug weltweit aktiv. Dabei kam die Verwaltung der Zugriffsrechte auf die File Server der Firma kaum noch mit dem Wachstum mit. Bis das IT-Team des Werkzeugherstellers Schritt für Schritt Ordnung in die Rechtevergabe brachte – mit vielen positiven Effekten.

Mit der Einführung der Software Liam, kurz für Light Identity Access Management, des Herstellers Consulting4IT gelang es Gedore, das Management von Laufwerkszugriffen nahezu vollständig zu automatisieren. Projektverantwortlicher war Frank Heisig, Teamleiter IT Infrastruktur beim Werkzeughersteller. Auslöser des Projekts waren der unverhältnismäßig hohe Aufwand im Umgang mit der bestehenden IT-Berechtigungsstruktur im Unternehmen, wie Heisig schildert: „Als ich bei Gedore anfing, habe ich nicht verwaltete File Server vorgefunden. Da gab es Berechtigungen auf jeder Ebene. Ohne Prozess, Struktur oder Transparenz. Klar, das ist bestimmt auch das Resultat einer gewachsenen IT-Struktur, wie es sie oft bei Familienunternehmen gibt. Irgendwann ist das eben nicht mehr verwaltbar. Für uns war das eine gute Gelegenheit, das Ganze einmal von Grund auf neu zu machen." Den Start des Projekts fasst er pragmatisch zusammen: „Wir haben den bestehenden Prozess gesehen, ihn eingerissen und einen Neuen aufgesetzt. Und dann haben wir mit einfachsten Mitteln losgeexcelt."

Von Excel zum ersten Tool

Frank Heisig, der damalige IT-Leiter Sven Tacke und sein Kollege Felix Kind, damals noch IT-Systemadministrator, entschieden sich für ein restriktives System, das die Rechtevergaben recht streng reglementierte, um Ordnung zu schaffen. Dazu wurden alle Daten auf neue Laufwerke migriert. Es wurde lediglich zwischen Projektlaufwerken und Teamlaufwerken unterschieden. Mit dem Microsoft-Bordmittel DFS (Distributed File System) schufen Heisig und Kind eine skalierbare, zentrale und international einsetzbare Struktur. Verwaltet wurde sie mit einer Excel-Vorlage. Heisig hatte diese so programmiert, dass am Ende ein Skript zur Verfügung stand, welches Ordner und Gruppen anlegte und auch berechtigte. Heisigs Kommentar zur damaligen Lösung: „Das war der erste Wurf und er stellte eine massive Produktivitätssteigerung dar. Aber der Verwaltungsaufwand dahinter war immer noch enorm." Doch mit dem Excel-System war die Grundlage für den Rollout eines Be-

rechtigungsmanagement-Toos entstanden. Heisig: „Wir haben nach der Excel-Lösung eine Software eingeführt, welche unsere grundlegenden Ansprüche erfüllt hat: Wir konnten damit die Rechte verwalten. Allerdings war die Anwendung im Grunde zu komplex für unsere Anforderungen und auch nicht besonders nutzerfreundlich. Als dann aufgrund der wachsenden Anzahl an Standorten auch noch die Änderungsanfragen massiv anstiegen, wurde uns klar, dass wir etwas anderes brauchten."

Bedarfsanalyse erstellt und verschickt

„Wir machten uns also Gedanken darüber, wie eine effektive Lösung aussehen könnte. Und kamen dann recht schnell darauf, dass eine Art Standardservice innerhalb unserer IT-Servicemanagement-Anwendung von Matrix42 ideal wäre. Ganz ohne Excel oder unnötige Komplexität, anwenderfreundlich und standardisiert. Ein Service, der unseren vollständigen Prozess abbildet, den jeder Anwender bei Bedarf eigenständig buchen kann und bei dem darüber hinaus auch noch alles sauber dokumentiert wird", fasst Heisig die Bedarfsanalyse zusammen. Da eine solche Anwendung im Standard des Matrix42 Service Catalog damals nicht existierte, wandten sich Heisig und Kind an den Matrix42-Spezialisten Consulting4IT. Dieser hatte bereits große Teile des Servicekataloges bei Gedore implementiert, sich aber auch einen Namen mit der Eigenentwicklung und dem Vertrieb von Matrix42-Add-ons gemacht. In den hauseigenen Trainings der Consulting4IT hatten die beiden außerdem bereits interessante Kontakte geknüpft und Ideen gesammelt. Heisig sendete dem IT-Dienstleister im Sommer 2019 die Anforderungen und eine Machbarkeitsanfrage zu. Noch heute zeigt er sich überrascht davon, wie schnell es danach ging: „Die Consulting4IT hat den Ball aufgenommen und bereits Ende 2019 ein Produkt geliefert: Liam."

Unklare Berechtigungen Adé

Heisig und Kind machten sich ans Werk, wobei sie versuchten, alles möglichst einfach aufzubauen. „Unser Kredo: Keep IT simple – IT muss einfach sein", erläutert Heisig die Philosophie hinter dem Projekt. Die Integration der Software in die Ordner- und Gruppenstruktur war in wenigen Stunden erledigt. Das Anlegen neuer Ordner und Berechtigungen im System wurde vom Dienstleister nach Vorgaben der Gedore-Mitarbeiter in wenigen Wochen erledigt. Die Struktur beruht auf dem Grundsatz, dass es zu jedem Ordner eine festgelegte Gruppe mit mindestens zwei Eigentümern gibt, die die Zugriffsrechte verantworten. Fragt nun ein Anwender über den Service nach einer Berechtigung, entscheidet einer dieser Eigentümer. Dabei wird der gesamte Vorgang im Hintergrund automatisch in einem Change dokumentiert. Seither gibt keine unklaren Berechtigungen mehr. Die Eigentümer können sich außerdem über eine Automation im Servicekatalog ausgeben lassen, wer alles Zugriff auf ihre Ordner hat.

Eigentümer mit Quotas

Eine weitere Funktion erwies sich als sehr nützlich: Die Verwaltung von Quotas, also einer Begrenzung des Speicherplatzes auf Speichermedien für Anwender oder Gruppen. „Das gab es bei uns in der Vergangenheit nicht und hat dazu geführt, dass mit dem Upload extrem großer Dateien versehentlich ganze File Server gesprengt wurden", erinnert sich Heisig. „Dafür gibt es eigentlich das integrierte Quota-Management von Windows. Aber das zu verwalten ist ein Graus." Mit einem von Gedore entwickelten und an das Zugriffsmanagement-System angedockten Tool können Anwender nun zusätzlich Quotas buchen. Werden 80 Prozent des erlaubten Speicherplatzes erreicht, werden sie vom System benachrichtigt und können mehr Speicherplatz beantragen. „So haben wir sichergestellt, dass unsere File-Ordner nicht mehr volllaufen", sagt Heisig.

Standorte einfach einbinden

Standorte einzubinden war früher ein Horrorszenario. Jetzt ist das innerhalb eines Tages erledigt. Wo in der Vergangenheit ein Admin viel Zeit und Aufwand investieren musste, ist es heute so einfach, dass der Aufbau eines File-Konstrukts für einen neuen Standort durchaus schon als Übung für Auszubildende genutzt wurde. „Aktuell binden wir viele Standorte an, weil wir unser IT-Einzugsgebiet massiv vergrößern", erzählt Heisig und erläutert den Prozess: „Heute muss ich der verantwortlichen Person vor Ort nur noch erklären, dass sie jetzt ein Dateneigentümer ist. Dann erkläre ich ihr, was sie in diesem Zusammenhang für Rechte und Pflichten hat: Das Recht, Zugriffsberechtigungen eigenständig zu erteilen und die Pflicht, diese zu verwalten und zu verantworten. Fertig. Damit geben wir den Menschen die Werkzeuge an die Hand, ihre Daten zu einem Großteil selbst zu migrieren." Heisig betont dabei nachdrücklich, dass das keinesfalls ein Abschieben von Arbeit sei. Von dem Prozess profitierten alle Beteiligten: „In der Regel ist dieses Vorgehen auch für den Datenverantwortlichen vor Ort einfacher. Denn bevor er wie früher der IT erklären muss, wie er seine Ordner angelegt haben will, läuft das über Liam viel schneller und außerdem automatisiert." Generell wurde das Tool von den Anwendern im Unternehmen gut angenommen, sagt Heisig.

Datenschutz und IT-Sicherheit

Die Zugriffsmanagement-Anwendung hilft auch dabei, die Anforderungen des Datenschutzes einzuhalten, Stichwort DSGVO. „Früher gab es ein wildes Rechtekonglomerat, das darauf beruhte, dass derjenige Zugriffsrechte bekam, der am lautesten schrie. Das ist ja per se eine Vorlage für DSGVO-Verstöße. Hier hätte ich nicht begründen können, warum wer irgendwelche Zugriffe hat", erläutert Heisig. „Das Risiko solcher Verstöße tendiert aufgrund der neuen Berechtigungsstruktur jetzt gegen Null. Sollte es doch einmal vorkommen, können Verstöße einfach erkannt, dem Datenschutzbeauftragten gemeldet und Gegenmaßnahmen eingeleitet werden." Das Tool reduziert auch das Risiko durch Insider-Bedrohungen, indem es interne Zugriffsrechte darstellt. Es agiert hier auf ähnlicher Grundlage wie die bei Gedore eingesetzte Security-Anwendung von Varonis. Deren Funktionsweise basiert ebenfalls auf der Untersuchung von Zugriffsrechten und internen Datenstrukturen. Heisig differenziert jedoch zwischen den beiden Softwares: „Liam gibt uns den Shop, verbessert den Service-Grad der IT und

spart uns viel Zeit und Kosten. Varonis hingegen deckt Ungereimtheiten, Fehler und Sicherheitslücken auf."

Vielfältige Nutzenaspekte

Die Systeme bringen Gedore auch an weiteren Stellen voran, wie die IT-Verantwortlichen schildern, etwa bei den Ein- und Austrittberechtigungen. „Das ist ein besonders schöner Beifang", sagt Heisig. Denn die Zugriffsmanagement-Anwendung kann im Fall eines Mitarbeiteraustrittes einen Report erstellen, der dessen Zugriffsberechtigungen anzeigt. Das erleichtert die Rechtezuordnung, wenn die Stelle neu besetzt wird.

Standard statt Customizing

Besonders erwähnenswert ist der hohe Standardisierungsgrad des Systems. „Wo früher jeder sein eigenes Süppchen gekocht hat, läuft heute alles gleich", schildert Kind und Heisig fügt hinzu: „Manchmal gibt es noch kleinere Probleme mit Microsoft-Bordmitteln, die zulassen, dass ab und zu Rechte überschrieben werden. Leider können wir das nicht ohne Weiteres umgehen. In der Regel passiert so etwas unbeabsichtigt, indem jemand Dateien ausschneidet und woanders wieder einfügt. Das überschreibt dann leider alle hinterlegten Berechtigungen. Früher war das ein Riesenproblem, da die Berechtigungen manuell aus einer Sicherung aufwendig wiederhergestellt werden mussten. Heute ist das Thema allenfalls noch lästig." Denn durch die Standardisierung lassen sich Berechtigungen per Klick neu setzen. Weitere Nutzenaspekte sind nach Heisig: „Die Software dokumentiert alles ITIL-konform in Changes und die Fehlerrate liegt im Promillebereich, wenn überhaupt. Und wenn der Chef mal wissen möchte, warum jemand einen bestimmten Zugriff hat, können wir ihm sofort Auskunft geben, ohne stundenlang Mails durchforsten zu müssen. Audits sind damit ebenfalls erledigt. Denn wir können nicht nur nachweisen, wer worauf Zugriff hat, sondern auch, wer wann auf was Zugriff hatte und wer das entsprechend genehmigt hat."

Berechenbarer ROI

Doch der entscheidende Nutzen stellt sich wohl bei den Kosten ein. Heisig rechnet vor: „Seit Start hatten wir insgesamt bis heute ca. 15.000 Änderungen in Berechtigungen. Bei im Schnitt drei Minuten Zeitaufwand pro Änderung und Admin und einem Kostensatz von etwa einem Euro pro Minute und Admin sind wir bereits bei 45.000 Euro Einsparung. Das entspricht 30 vollen Admin-Tagen im Jahr. Dabei sind Ticketbearbeitung und Dokumentation noch gar nicht mitberücksichtigt. Und die Zahlen sind voll skalierbar. Wenn man das also auf ein größeres Unternehmen mit weit mehr als unseren aktuell 600 Usern überträgt, kann man sich ausrechnen, welch immenses Einsparungspotenzial man damit erreicht."

Das Konzept als Erfolgsfaktor

Trotz der Komplexität des Projekts lief es von Beginn an nahezu reibungslos und die Zusammenarbeit mit dem Dienstleister war produktiv. „Anfangs haben wir zum Teil etwas aneinander vorbeigesprochen", räumt Felix Kind ein, „aber das waren Kleinigkeiten." Bugs wurden schnell behoben, neue Features in wenigen Tagen implementiert. "Neben dem Tagesgeschäft alle Neuerungen zu verarbeiten, war manchmal schon eine ordentliche Aufgabe", sagt Kind. Zurückzuführen ist dieser Projekterfolg vor allem auf die gute Vorarbeit bei Gedore. Vor Einführung des Tools räumte die Firma ihre File-Server-Ebene restriktiv auf, immer anhand des Konzeptes. Heisig: „Ich brauche ein Berechtigungskonzept, das logisch und damit automatisierbar ist. Wenn ich hingegen darauf bestehe, in fünf verschiedenen Ebenen Gruppen berechtigen zu müssen – was in der Software möglich wäre – wird mir das Projekt mit viel Freude ins Gesicht schlagen. Wenn ich das Ganze jedoch so vereinfache, dass ich es auf einer DIN A4 Seite beschreiben kann, dann hat es die besten Erfolgschancen. Auch hier wieder: IT muss einfach sein!" Heisigs Tipp: Das Konzept sollte an Standards ausgerichtet sein, eine durchdachte Eigentümer-Struktur, definierte Schreib- und Leserechte sowie eine durchgängige Namenskonvention haben. Weiter sei es sinnvoll, hauptsächlich mit Einzelberechtigungen zu arbeiten, da die Anwendung einen darauf ausgerichteten Service bereit stellt.

Weitere Projekte geplant

Aktuell migriert der Werkzeughersteller weitere Altdaten, die aus der Zeit vor der Systemeinführung stammen. Für die Zukunft gibt es auch schon weitere Ideen. Denn der Hersteller möchte die Logik seiner Files Shares auch bei seinen Shared Mailboxes, bei Microsoft Teams und Sharepoint anwenden. So ergibt sich heute folgendes Bild bei Gedore: Aus dem Sorgenkind File Server ist eine standardisierte und automatisierte IT-Plattform geworden. Die Verantwortung wurde in den Fachbereich verlagert, der am besten über die Vergabe von Rechten entscheiden kann. Da sich das Zugriffsmanagement-System im Standard der Matrix42-Software bewegt, sind Stabilität und Update-Sicherheit hergestellt. Und weil die Anwender Berechtigungen untereinander beantragen und vergeben, bleibt der IT mehr Zeit für andere Projekte. Das Grundprinzip 'Keep IT simple' zahlt sich aus. ■

Linda Schmittner ist PR Managerin und Autorin bei der Consulting4IT GmbH.

www.consulting4it.de

Bild: Gedore Werkzeugfabrik GmbH & Co. KG