Das britische Parlament optimiert die Verwaltung von Active Directory (AD)

UK Parliament Digital Service

PDS vereinfacht mit Active Roles die Verwaltung von Active Directory, steigert die Sicherheit und setzt Zeit für die Hybrid-Cloud-Migration frei

Kunde:

Parliamentary Digital Service (PDS)

Branche:

Öffentlicher Sektor – Regierung

Land:

Vereinigtes Königreich

Webseite:

www.parliament.uk

Herausforderung

- Jeden Monat Stunden an Zeitverlust aufgrund der ineffizienten Verwaltung von Neuzugängen, Stellenwechslern und Ausscheidern (Joiners, Movers und Leavers, JML)
- Höheres Risiko durch die manuelle Kontrolle des Privileged Access Management (PAM)
- Fehlende Unterstützung für die Hybrid Cloud

Die Lösung

- One Identity Active Roles

- Mehr Zeit für die Durchführung strategischer Migrationsprojekte
- Automatisierung von JML-Prozessen und PAM zur Verbesserung von Schutz, Effizienz und Sicherheit
- Bewältigung von Lizenzierung-sproblemen bei Zoom-Konferenzen während der Pandemie
- Förderung der Integration mit Active Directory und Azure Active Directory

Parliamentary Digital Service (PDS) unterstützt das britische Unterhaus und Oberhaus sowie parlamentarische Mitarbeiter. Zu den vielfältigen Aufgaben von PDS gehört die Unterstützung der IT, die Verwaltung des Netzwerks des Parlaments, die Entwicklung von Anwendungen und die Planung des zukünftigen Technologiebedarfs. Darüber hinaus betreibt PDS auch die Webseite und die Social-Media-Präsenzen des britischen Parlaments.

Das Unterhaus und Oberhaus des britischen Parlaments ziehen nicht nur große Touristenmassen an, sondern sind auch ein beliebtes Ziel von Cyberkriminellen, die sich in noch größeren Mengen um das Netzwerk des Parlaments scharen. „Die Sicherheitsbedrohungen nehmen kein Ende“, sagt Cherry O’Donnell, Leiterin für Identitäts- und Zugriffsmanagement bei PDS. „Wir sind ein wichtiges Ziel. Deshalb hat die Netzwerksicherheit bei uns oberste Priorität.“

Verwaltung mehrerer Änderungen

Es ist keine leichte Aufgabe, durch eine sorgfältige Zugriffsverwaltung für die Sicherheit eines Netzwerks zu sorgen. Dabei steht PDS aufgrund der hohen Anzahl und Vielfalt der Konten in Active Directory (AD) vor einer Herausforderung.

Zum einen sind die Konten der Abgeordneten des Unterhauses und ihres Personals, sowie der Mitglieder des Oberhauses und ihrer Mitarbeiter zu verwalten. Zum anderen beschäftigt das Parlament über 2.000 ständige Mitarbeiter, von denen jeden Monat 100 bis 200 zum Netzwerk hinzukommen oder dieses verlassen. Für diese Benutzer müssen Konten erstellt oder gelöscht werden. Zudem müssen die AD-Gruppen für die zahlreichen bestehenden Netzwerkbenutzer, die neue parlamentarische Positionen übernehmen, aktualisiert werden. Innerhalb der AD-Gruppen gibt es wiederum privilegierte Konten, die PDS kontrollieren muss, damit Administratoren für Aufgaben wie das Aufspielen von Patches Zugriff auf die Hardware, einschließlich der Server, erhalten.

> „Mit One Identity Active Roles haben wir einen **klaren Überblick** darüber, wer zu einem bestimmten Zeitpunkt **Berechtigungen** hat oder in der Vergangenheit Berechtigungen hatte. Es gibt keinen **Raum für Fehler**.“
>
> Cherry O’Donnell, Leiterin für Identitäts- und Zugriffsmanagement, PDS

Zeitaufwendige Aufgaben

Die Verwaltung von Neuzugängen, Stellenwechslern und Ausscheidern (Joiners, Movers und Leavers, JML) sowie die Kontrolle des Privileged Access Management (PAM) erfolgte in AD größtenteils manuell. Dies nahm jeden Monat viele Stunden in Anspruch, die das Team von PDS für strategische Projekte hätte nutzen können. Der Mangel an Automatisierung war mit einem größeren Risiko für menschliche Fehler verbunden und es bestand eine größere Wahrscheinlichkeit, dass sich jemand unbefugten Zugriff auf Informationen verschaffen konnte. Darüber hinaus war die alte Lösung für

„Wir sparen Stunden an Zeit, sodass wir Initiativen wie den Plattformwechsel zu Active Roles 7.4. vorantreiben können.“

Cherry O’Donnell, Leiterin für Identitäts- und Zugriffsmanagement, PDS

Zugriffsmanagement nicht für Azure AD und eine Hybrid-Lösung optimiert, die eine lokale mit einer Cloud-basierten AD-Umgebung kombiniert.

PDS beauftragte One Identity damit, die Verwaltung und Sicherheit für eine hybride AD-Infrastruktur zu verbessern. Die Organisation verfügte über eine ältere Version von One Identity Active Roles und wollte ihre Lösung optimieren, um von den neuesten Innovationen des Produkts zu profitieren. PDS nahm mit der Unterstützung des Teams von One Identity die Verbesserung in Angriff. Dabei wurden Tausende von Zeilen an Befehlszeilenshell und Skriptsprache durch Active Roles mit Powershell-Modulen und Active Roles-Workflows ersetzt. „Ein Berater von One Identity hat uns unterstützt“, so O’Donnell. „Wir haben alle wirklich hart an dem Projekt gearbeitet und unsere gesteckten Ziele erreicht.“

Jeden Monat Stunden an Zeiteinsparungen beim Zugriffsmanagement

Die JML-Verwaltung in AD ist jetzt voll automatisiert, sodass das Identitäts- und Zugriffsmanagementteam wertvolle Zeit wiedergewinnt. Hierzu meint O’Donnell: „Wir sparen Stunden an Zeit, sodass wir Initiativen wie den Plattformwechsel zu Active Roles 7.4 vorantreiben können. Da wir Stunden an Zeit einsparen, können wir uns jetzt auf wichtige Aufgaben wie die Bedrohungsanalyse konzentrieren. Heute frage ich mich, wie wir es in der Vergangenheit geschafft haben, unsere Arbeit zu erledigen.“ Wenn ein neuer Mitarbeiter anfängt oder jemand das Unternehmen verlässt, werden keine E-Mails mehr verschickt, in denen der Kontozugriff oder die Kontobeendigung angefragt wird. Dank Integrationen mit der Personal-abteilung werden Daten zu Neuzugängen, Stellenwechslern und Ausscheidern an Active Roles weitergegeben und Konten werden automatisch aktiviert oder beendet. „Neue Mitarbeiter haben von Anfang an Zugriff auf grundlegende Services wie E-Mail und OneDrive. Sie rufen uns zur Kennwort-einrichtung an und sind dann sofort einsatzbereit“, so O’Donnell.

Nahtloser und sicherer privilegierter Zugriff

PDS hat außerdem PAM automatisiert. Dabei wird für den Zugriff auf Server für Aufgaben wie das Aufspielen von Patches ein Zeitlimit festgelegt. „Wenn die für eine Aufgabe zugewiesene Zeit abgelaufen ist, entzieht Active Roles automatisch die Berechtigung“, sagt O’Donnell. „So besteht nicht die Gefahr, dass jemand es vergisst.“ PDS stellt auf ein Zero Trust-Modell um, bei der jeder administrative Vorgang eindeutig authentifiziert wird. Gegenwärtig ist PAM jedoch einfach und Administratoren können Berechtigungen über ein Webportal mit Dropdown-Menüs anfordern. Active Roles generiert

die Berechtigung, sofern die Aufgabe nicht so vertraulich ist, dass sie von O'Donnell oder einem anderen leitenden Mitarbeiter von PDS autorisiert werden muss.

Sobald eine Berechtigung gewährt wird, erhalten das Cybersecurity-Team und das Identitäts- und Zugriffsmanagementteam von PDS eine E-Mail, damit alle Rechteerweiterungen sichtbar sind. Darüber hinaus werden in Active Roles Zugriffsprotokolle generiert, die von Auditoren bei Bedarf abgerufen werden können. „Mit One Identity Active Roles haben wir einen klaren Überblick darüber, wer zu einem bestimmten Zeitpunkt Berechtigungen hat oder in der Vergangenheit Berechtigungen hatte", sagt O'Donnell. „Es gibt keinen Raum für Fehler."

Wirksame Maßnahmen gegen die Pandemie

PDS hat dem britischen Parlament mithilfe von Active Roles außerdem ermöglicht, effektiv auf die Pandemie zu reagieren. Abgeordnete des Unterhauses und Minister der britischen Regierung haben für Diskussionen und Debatten die Videokommunikation über Zoom genutzt. Da die Anzahl der Zoom-Lizenzen des britischen Parlaments jedoch begrenzt ist, muss PDS den Zugriff sorgfältig verwalten. „Wir erstellen ein von Active Roles unterstütztes Webformular", erklärt O'Donnell. „Im Formular wird der Name und das Datum der Diskussion oder Debatte angegeben und Active Roles fügt den Abgeordneten oder Minister zur AD-Gruppe für Zoom hinzu. Der Zugriff wird dann zum Tagesende automatisch wieder aufgehoben."

Zugriffsmanagement vollständig in der Cloud

Das Team von PDS freut sich auf die Einführung von Active Roles 7.4. „Es ist rein Cloud-basiert", sagt O'Donnell. Wir werden in der Lage sein, in einem einzigen Workflow Benutzer in der Cloud anzulegen und ihnen Zugriff auf SharePoint und One Drive zu gewähren. Dies ist eine echte Komplettlösung." Für O'Donnell sind die Verbesserungen in 7.4 Ausdruck der Kundenorientierung von One Identity. „Technologie bietet uns neue Möglichkeiten und schafft gleichzeitig neue Risiken", merkt sie an. „One Identity bietet die Tools, mit denen wir den größten Nutzen daraus ziehen können, und schützt uns gleichzeitig vor den Nachteilen. So haben wir von Anfang an ein Gefühl der Sicherheit."

Über One Identity

Das Quest Software-Unternehmen One Identity ermöglicht es Unternehmen, lokal, in der Cloud oder in einer Hybrid-Umgebung eine identitätszentrierte Sicherheitsstrategie zu implementieren. Unser einzigartig breites und integriertes Portfolio mit Angeboten zur Identitätsverwaltung umfasst Kontoverwaltung, Identity Governance und Administration sowie Privileged Access Management. Weitere Informationen erhalten Sie unter OneIdentity.com.