



Maas & Waal Care Group

reduzierte Anfragen zum Zurücksetzen von Passwörtern von 400 pro Monat auf zwei pro Woche.

Executive Summary

KUNDE

Maas & Waal Pflegegruppe

AUFGABE

Um passwortbezogene Anfragen zu reduzieren und das Pflegepersonal selbstständiger zu machen, suchte die Maas and Waal Pflegegruppe nach einer Möglichkeit, die Authentifizierung und das Passwortmanagement zu zentralisieren.

LÖSUNG

Active Directory dient als zentrale Authentifizierungsquelle für alle lokalen und Cloud-Anwendungen unabhängig vom Authentifizierungsmechanismus und wird durch ein Self-Service-Passwort-Portal ergänzt, damit Mitarbeiter ihr Passwort 24 Stunden am Tag, 7 Tage die Woche zurücksetzen können.

PRODUKT

HelloID, E-SSOM, SSRPM

ERGEBNIS

Die Häufigkeit der Passwort-Rückstellungsanfragen von Maas & Waal sank um 98% von 400 pro Monat vor der Implementierung, wodurch sowohl die Frustration der Mitarbeiter als auch die der Helpdesk-Mitarbeiter minimiert wurde.

Die Maas & Waal Care Group (zMW) bietet ein komplettes Dienstleistungspaket rund um Pflege, Wohnen und Soziales im Land van Maas en Waal. Die 800 Mitarbeiter des ISO-zertifizierten Unternehmens arbeiten in fünf Zentren, um den Kunden rund um die Uhr eine Betreuung zu gewährleisten. Die Mitarbeiter benötigten eine Vielzahl von Passwörtern, um Zugang zu ihren Pflegeanwendungen zu erhalten, was zu einer komplexen und zeitaufwändigen Verwaltung sowohl für Benutzer als auch für Administratoren führte. Um diese Probleme zu lösen, implementierte zMW das Access Management Portal von Tools4ever: HelloID.

Marco Peters, IT-Koordinator von Maas & Waal, machte sich mit dem wachsenden Passwortproblem im Gesundheitswesen vertraut: „Anwendungen haben eigene Passwortrichtlinien, um die Sicherheit zu gewährleisten. Leider stimmen die verschiedenen Passwortregeln nicht überein. Das schafft schnell Verwirrung und Frustration bei den Mitarbeitern.“ Die Authentifizierungs- und Passwortregeln werden von den Anwendungsanbietern durchgesetzt. Die Ablaufpläne der verschiedenen Passwörter verursachten bei den Endbenutzern eine besondere Frustration. „Die Benutzergruppe ist sehr erfahren im Bereich der Pflege, hat aber weniger Affinität zu Computern und IT.“ Die Reduzierung der Anzahl der Passwörter mit HelloID & E-SSOM macht es für die Mitarbeiter leicht zu verstehen. Das zentrale, benutzerfreundliche Portal von HelloID ermöglicht den Zugriff über Office Desktops, Chromebooks oder sogar von zu Hause aus.

Cloud-Anwendungen über Active Directory-Anmeldeinformationen „Das IT-Management ist für die IT verantwortlich. Infrastruktur, 45 Anwendungen, VOIP-Systeme, WLAN und das Management der Glasfaserverbindungen. Wir sind auch für die Healthcare-Domotik verantwortlich.“ Ohne genügend Zeit, um beides zu erörtern, müssen sich Maas & Waal's IT-Administratoren oft zwischen ihren Bemühungen auf die Wiederherstellung von Passwörtern konzentrieren oder die Verwaltung der Technologieumgebung.

„Wir konnten die Einsparungen sofort transparent machen und die Organisation wollte diese Lösung beibehalten.“

Marco Peters, IT Coordinator

Während größere Projekte oder Urlaubszeiten, gab es täglich im Durchschnitt 20 Rücksetzanforderungen, sodass externe Manager um Hilfe gebeten wurden, aber die Arbeitsbelastung war dennoch sehr hoch und zu viel. „Unglücklicherweise passierte es, dass ein Passwortticket erst nach ein paar Tagen bearbeitet wurde“, fuhr Marco Peters fort.

Jetzt können sich Mitarbeiter mit ihrem Active Directory-Anmeldeinformationen (AD) in die HelloID App einloggen und sofort und ohne Zeitverzögerung sicher auf Anwendungen wie YouForce, Planywhere, Outlook Webmail, Qic, SharePoint und UKON zugreifen.

PASSWORT-RÜCKSETZUNG DURCH DEN BENUTZER SELBST

Über HelloID dienen AD-Konten als Identität für alle Anwendungen. Darüber hinaus ermöglicht Self-Service Reset Password Management (SSRPM) den Mitarbeitern, diese AD-Anmeldeinformationen jederzeit selbst sicher zurückzusetzen. Die Mitarbeiter müssen nicht mehr auf die IT warten und können über eine Webseite oder den Windows-Anmeldebildschirm zum Reset-Portal navigieren. Sicherheitsfragen und Antworten bieten Verifizierungsschritte, bevor der Benutzer Werte ändern kann. Auch wenn das Konto gesperrt ist, kann der Benutzer es selbst entsperren.

GRÖSSTE HERAUSFORDERUNG

Marco Peters: „Die Passwortverwaltung ist seit Jahren ein Problem. Die Herausforderung bestand darin, das Management von einer Investition in eine Lösung zu überzeugen, zumal die Budgets immer weiter schrumpfen. Ich habe endlich den Schritt gemacht, den Piloten mit Tools4ever zu starten, woraufhin (alle) sofort den Nutzen sahen. Ich hätte das viel früher tun sollen.“

VORTEILE

- **Active Directory dient als primäre Authentifizierungsquelle**
- **Passwort-Rücksetzung rund um die Uhr möglich**
- **Single Sign-On für alle Anwendungen**
- **Melden Sie sich einfach und schnell bei Cloud-Anwendungen an**
- **Die IT kann sich auf Großprojekte konzentrieren und die Mitarbeiter können effizienter arbeiten**
- **Zentrale Verwaltung und Kontrolle über die Passwortverwaltung**
- **Schnelle Implementierung und direktes Ergebnis**

ERGEBNIS

Durch die Zentralisierung des Passwortmanagements steuert die IT-Abteilung von Maas und Waal die verschiedenen Passwortanforderungen und den Authentifizierungsprozess. Die Authentifizierung der Mitarbeiter erfolgt über Active Directory (AD) unabhängig von der Anwendung. Dies gilt sowohl für Windows (Client-)Anwendungen als auch für (Online-)Webanwendungen. Mitarbeiter werden nicht mehr mit unterschiedlichen Passwörtern und unterschiedlichen Ablaufdaten konfrontiert. Jetzt können sich die Administratoren auf Wartung und Projekte konzentrieren, und die nächtlichen Reset-Aufrufe wurden eliminiert, so dass die Mitarbeiter in der Lage sind, ihre eigenen Resets durchzuführen. Passwort-bezogene Tickets sind auf nur noch 2 pro Woche gesunken. Der durchschnittliche Turnaround für einen Reset ist