

SICHER UND STETS BEREIT ZUM AUDIT

# Identitäts- und Zugriffsmanagement im Healthcare-Sektor

## Unternehmen

*Star-shl, führender niederländischer Anbieter medizinischer Dienstleistungen, beschäftigt 1.300 Mitarbeiter an verschiedenen Standorten. Die Mitarbeiter von Star-shl unterstützen und beraten Fachleute wie Allgemeinmediziner, Hebammen, Krankenhäuser und Gesundheitseinrichtungen in den südwestlichen Niederlanden. Das Unternehmen ist spezialisiert auf Laboruntersuchungen von Blut-, Urin- und Stuhlproben sowie auf bildgebende Verfahren und Funktionstests wie Röntgen oder Ultraschall. Star-shl nutzt digitale Technologie, um den Datenfluss und ein logistisches Netzwerk zwischen den beteiligten Diagnosezentren, Laboren und Forschungseinrichtungen zu ermöglichen. Da das Unternehmen mit sensiblen Patientendaten arbeitet, steht es unter genauer Beobachtung mit entsprechend häufigen Audits.*



## AUSGANGSSITUATION

### Vom Plan, ein eigenes Portal zu entwickeln

Die IT-Spezialisten von Star-shl hatten schon seit einiger Zeit Abfragen und andere Aufgaben innerhalb von Active Directory mit PowerShell automatisiert. Die Identitäts- und Zugriffsverwaltung war zeitaufwändig und beinhaltete eine Menge manueller Aufgaben und Excel-Tabellen. Das Team wollte die Automatisierung mit PowerShell weiter vorantreiben und suchte eine benutzerfreundlichere Option als die Verwendung der PowerShell-Befehlszeile. Die Erstellung einer eigenen grafischen Benutzeroberfläche aus dem Nichts erwies sich jedoch als zeitaufwändig und führte nicht zum gewünschten Ergebnis.

### Schon in der ersten Woche einsatzbereit?

Ein selbst erstelltes Portal brachte nach der vorgegebenen Zeit nicht die erwünschten Ergebnisse. Daher beschloss das Team bei Star-shl, eine Lösung von der Stange auszuprobieren. Aber würde ScriptRunner so schnell einsatzbereit sein wie versprochen? Würde es die branchenspezifischen Sicherheitsanforderungen erfüllen? Würde die Software das Identitäts- und Zugriffsmanagement erleichtern und den Umgang mit Mitarbeiterdaten und ihren verschiedenen Zugriffsrechten etc. vereinfachen?

## LÖSUNG

### Active Directory – erste Anwendungsfälle

Das Herzstück des Identitäts- und Zugriffsmanagements von Star-shl sind die Berechtigungsprofile. Jede Änderung bestehender Benutzer oder das Anlegen eines neuen Kontos bedeutete, dass die Personalabteilung per E-Mail oder telefonisch einen Helpdesk-Mitarbeiter mit Informationen versorgen musste, Excel-Tabellen gegengeprüft wurden, Konten zugeordnet oder manuell angelegt wurden. Insgesamt gab es viel Potenzial durch Automatisierung Zeit zu sparen und die Datenqualität und -konsistenz zu verbessern.

Die ersten Anwendungsfälle für ScriptRunner bezogen sich also alle auf Active Directory. Es wurden Actions entwickelt, um das System automatisch auf vorhandene IDs zu überprüfen, Konten zu erstellen oder die Mitgliedschaft in einer Sicherheitsgruppe zu ermöglichen. Prozesse wie das Onboarding neuer Kollegen, die Archivierung inaktiver Postfächer, die Verwaltung von Zugriffsrechten während der Beschäftigung oder die Deaktivierung von Konten beim Offboarding wurden vereinfacht. Sobald eine Aktion eingerichtet ist, kann sie manuell, automatisch (nach einem Zeitplan) oder durch ein anderes System ausgelöst werden – bei Star-shl ist dieses System Jira Service Desk, die Helpdesk-Software von Atlassian.

### Häufige Passwortänderungen managen

Aufgrund erhöhter Sicherheitsanforderungen müssen die Mitarbeitenden bei Star-shl ihre Passwörter mit einer bestimmten



Warum sollte ich etwas manuell erledigen, wenn ich es mehr als einmal durchführen muss?

Axel Haringa, Senior IT Specialist



Häufigkeit ändern. Um diesen Prozess deutlich zu erleichtern, erstellten die IT-Spezialisten ScriptRunner Actions, mit denen Passwortänderungen möglich sind, ohne Zugriff auf Active Directory zu gewähren: Die eine Option ist ein Webportal, über das Mitarbeitende selbstständig ihr Passwort zurücksetzen können, was durch eine Bestätigung per Mobiltelefon abgesichert wird.

Die andere Option ist über die Helpdesk-Kolleg:innen. Das führende System im Helpdesk bei Star-shl war und ist Atlassian Jira, aber jetzt ist Jira über die REST-API verbunden und kann Actions in ScriptRunner auslösen. Wenn ein bestimmtes Kontrollkästchen aktiviert ist, löst Jira die Action „Passwort ändern“ aus. Die spezifische Änderung an Active Directory wird ausgeführt, ohne dass administrative Rechte am System erforderlich sind. Dabei ist es wichtig, die Anzahl von Personen mit administrativen Rechten in Active Directory zu begrenzen, da dies die Datensicherheit erhöht und dazu beiträgt, potenzielle Sicherheitsprobleme zu minimieren.

Beim Umgang mit Daten – insbesondere im Gesundheitswesen – ist Datenschutz von zentraler Bedeutung. Bei der Verwendung von ScriptRunner kann ein Helpdesk- oder ein Endbenutzer Actions auslösen, ohne auf die Systeme zugreifen zu müssen. Die zur Durchführung der jeweiligen Action erforderlichen Anmeldeinformationen werden sicher gespeichert.

### Erforderliche Audits für die Zertifizierung nach NEN 7510

Der Gesundheitssektor wird streng überwacht. NEN, das Königliche Niederländische Normungsinstitut, spezifiziert die Anforderungen an die Informationssicherheit in der Norm NEN 7510 (vergleichbar mit ISO 27001). Jährliche Audits sind obligatorisch. Nachdem ScriptRunner eine Zeit lang im Einsatz war, stellten die IT-Spezialisten fest, dass die Software es Star-shl ermöglicht, stets konform und jederzeit bereit für ein Audit zu sein. Axel Haringa, Senior IT Specialist, weist stolz darauf hin: „Änderungen am System sind nachvollziehbar. Die Auditoren sind mit unserem System sehr zufrieden.“

Das Zugriffgewähren auf einzelne Actions statt auf komplette Systeme hat sein Leben vereinfacht. Sicherheitsprobleme, die durch unzureichende Dokumentation, mangelndes Wissen oder kleine Pannen bei der Arbeit mit komplexen Systemen entstehen, gehören nun der Vergangenheit an.

### Automatisiertes Identitäts- und Zugriffsmanagement wird zum Erfolg

Axel Haringa spricht ganz offen: „Die Automatisierung unseres Identitäts- und Zugriffsmanagements hat Zeit gekostet und war ein ziemlicher Prozess. Aber wir verwalten jetzt 1.300 Mitarbeiter sicher – vom Onboarding bis zum Offboarding und allem, was dazwischen liegt.“

Der gesamte Lebenszyklus der Mitarbeitenden wurde analysiert, und Schritt für Schritt kamen Actions hinzu. Das Schöne daran ist: Wann immer jemand Automatisierungspotenzial sieht, können neue Skripte erstellt und Actions hinzugefügt werden; die Software ist flexibel und schreibt keine bestimmten Prozesse vor. Außerdem war es für Star-shl wichtig, dass alle Daten vor Ort bleiben. Star-shl hat die volle Kontrolle über ihren -Server, so wie sie zum Beispiel auch Active Directory oder Exchange auf ihren eigenen Servern betreiben. Wenn eine Action in ScriptRunner ausgelöst wird, wird ein separater PowerShell-Prozess gestartet. An diesen Prozess werden das Skript, alle Parameter und andere erforderliche Informationen übergeben. Im lokalen Modus erfolgt die gesamte Skriptverarbeitung lokal.

### Queries – klein aber oho

Queries (Abfragen) haben sich als besonders hilfreich erwiesen. Durch Queries können Daten aus verschiedenen Datenbanken abgerufen werden. Auf diese Weise lassen sich beispielsweise die Actions einschränken, die eine Person ausführen darf, oder die Gruppe definieren, der ein Star-shl-Mitarbeitender hinzugefügt werden darf. Jede Aktion kann aus verschiedenen Queries und Targets (Abfragen und Zielsystemen) bestehen. Das Ergebnis einer Query bestimmt z. B., welche Auswahlmöglichkeiten ein Benutzer erhält oder welcher Teil der Infrastruktur sichtbar und zugänglich ist, wenn eine bestimmte Action ausgelöst wird. Mit einem Query-Skript kann eine dynamische, interaktive Auswahl für Parameterwerte erstellt werden.

---

**„Die Verwendung von Queries ist ein starkes Argument für ScriptRunner! Man kann Personen oder ganzen Abteilungen genau die richtigen Auswahlmöglichkeiten geben, nicht mehr und nicht weniger.“**

---

Queries scheinen auf den ersten Blick kein großes Ding zu sein zu sein, aber sie sind nach Meinung von Axel Haringa nicht zu unterschätzen. Die Actions, die bei Star-shl entwickelt wurden, verwenden Queries, um die Auswahlmöglichkeiten einzuschränken, die Benutzer aus verschiedenen Abteilungen oder Helpdesk-Kollegen haben. Die Actions, die sie erstellt haben, können Aufgaben wie die Verteilung von Softwarelizenzen lösen – ein Beispiel dafür ist die Zuweisung oder der Entzug einer GoToMeeting-Lizenz. Ein anderes Beispiel ist der Neustart eines bestimmten Dienstes, ohne dass dabei versehentlich ein Dienst heruntergefahren wird, der einwandfrei lief.

### Komplexe Systeme nahtlos integrieren

Active Directory, Exchange On-Premises, Windows-Server, Citrix Virtual Desktop, Atlassian Jira, andere Datenbanksysteme, branchenspezifische Legacy-Software – bei Star-shl sind verschiedene



Die Leute denken entweder nicht über Automatisierung nach – oder sie zögern, Skripte und eine Befehlszeile zu verwenden, sondern nutzen lieber eine grafische Benutzeroberfläche.

Axel Haringa, Senior IT Specialist



Systeme im Einsatz und eine nahtlose Integration ist erforderlich. Die IT-Spezialisten schätzen besonders, dass PowerShell-Skripte so vielseitig einsetzbar sind. Alle Zielsysteme, für die PowerShell-Module verfügbar sind, können von ScriptRunner bedient werden. Über Konnektoren können weitere Drittsysteme an ScriptRunner angebunden werden, was die Plattform funktional erweitert.

### VMware – Potenzial für mehr Automatisierung

Auf die Frage, wann er seinen größten Aha-Moment hatte, fallen Axel Haringa einige Dinge ein, die heute reibungslos laufen, aber früher sowohl nervenaufreibend als auch sehr zeitintensiv waren. Die Installation und Konfiguration von Microsoft SQL-Servern dauerte früher mehrere Stunden und erstreckte sich über zwei oder drei Tage. Jetzt dauert der gesamte Prozess nur noch 1,5 Stunden. Sein Ziel ist es, den Prozess weiter zu optimieren und schließlich einen vollständig konfigurierten SQL-Server innerhalb von nur 10 Minuten zum Laufen zu bringen.

Die IT-Spezialisten von Star-shl erstellen und verknüpfen bereits Berechtigungsgruppen aus Active Directory mit Computerobjekten in VMware. Aber das ist noch nicht alles: „Ich arbeite auch an einem Skript, um die Erstellung und Initialisierung von Festplatten, das CD-Mounting und Reboots über VMware zu verwalten“, erwähnt Axel Haringa.



## ERGEBNIS

Axel Haringas Motto bei der Arbeit ist: „Warum sollte ich etwas manuell erledigen, wenn ich es mehr als einmal durchführen muss?“ Die vollständige Automatisierung des Identitäts- und Zugriffsmanagements vom Onboarding bis zum Offboarding und allen dazwischen liegenden Änderungen war sicherlich ein Kraftakt, aber die Arbeit hat sich gelohnt, der Zeitaufwand für diese Prozesse wurde maßgeblich verringert. Doch bei der Automatisierung geht es nicht nur um Zeitersparnis. Wiederkehrende Aufgaben werden jetzt auf die gleiche Weise und mit der gleichen Ergebnisqualität ausgeführt. Änderungen am System sind transparent, was die Auditoren freut. Das Risiko, versehentlich auf Daten zuzugreifen, diese zu gefährden oder einen bestimmten Dienst unbeabsichtigt abzuschalten, wurde verringert. Actions können delegiert werden, ohne dass administrative Rechte erteilt werden müssen. Mehr Sicherheit (und weniger Notfälle) im Betrieb der IT-Infrastruktur entlastet die Administratoren, sie können unter weniger Stress arbeiten und haben mehr Zeit für Automatisierung und sinnvolle, befriedigende Aufgaben.

## KEY FACTS

- Vernetzte Systeme: Helpdesk-Mitarbeiter nutzen Atlassian Jira, um Aktionen in ScriptRunner auszulösen.
- Sicherheit: Aktionen können ausgeführt werden, ohne dass ein vollständiger administrativer Zugriff erforderlich ist.
- Konform und bereit zum Audit: Änderungen am System sind nachvollziehbar.
- Queries: Leistungsstark, um genau festzulegen, was ein Benutzer sehen darf.