Whitepaper HelloID

Identity as a Service (IDaaS)

TOOLS4EVER
IDENTITY GOVERNANCE & ADMINISTRATION

Inhaltsverzeichnis

Trends im Identity Management

Identity-Management-Software spielt in vielen IT-Umgebungen seit langem eine zentrale Rolle. Mit dieser Funktionalität erhalten die Benutzer Zugang zu ihrer IT-Umgebung und können ihre Anwendungen und Daten nutzen. Mit Trends wie der zunehmenden Digitalisierung und der weiteren Entwicklung der Cloud verändern sich auch die Anforderungen an Identity-Management-Software. Im Folgenden beschreiben wir diese Trends und was sie für die IDM-Funktionalität bedeuten.

Trend	Folge
Unternehmen stellen auf die Cloud um. Grundlegende Infrastrukturkomponenten wie Exchange, Active Directory und lokale Datenträger werden auf Azure, Office 365 und Teams umgestellt. Unternehmensanwendungen wie das HR-System wurden oft schon früher in die Cloud migriert. Das eigene Rechenzentrum wird nur bis zum Ablauf der Abschreibungsfrist parallel weiterbetrieben, die Infrastruktur sukzessive ersetzt.	I**AM-Systeme werden durch IDaaS-Software (Identity as a Service) ersetzt.** In einigen Jahren werden Unternehmen keine lokale Infrastruktur mehr haben. Auch die Identity- und Access-Management-Lösung muss dann als Dienst verfügbar sein. Diese Systemlösungen werden als Identity as a Service (IDaaS) bezeichnet und bieten als Cloud-Dienste eine bessere Betriebszeit, niedrigere Kosten und nahtlose Updates.
Daten über Produkte, Kunden und Mitarbeiter werden immer wertvoller, aber auch immer stärker reguliert. Der schnelle, vollständige und korrekte Zugriff der Mitarbeiter auf diese Daten ist ein immer wichtigerer Erfolgsfaktor für Unternehmen. Die verschärften Gesetze und Vorschriften (DSGVO, BDSG, Meldepflicht für Datenlecks) zwingen Unternehmen zu weitreichenden Maßnahmen, um negative Audits, Bußgelder und Imageverlust zu verhindern.	**Sicherheitsmaßnahmen und Audit-Compliance muss auf der untersten Ebene angesetzt werden: Identity.** Früher reichten halbautomatische Verfahren und einige wenige Skripte aus, um Daten zu schützen und die geltenden Anforderungen zu erfüllen. Dies wird jedoch immer schwieriger. Vorstand, Aufsichtsrat und Sicherheitsbeauftragte fordern zunehmend eine unternehmensweite professionelle IDaaS-Lösung.
Automatisierung und Effizienz haben höchste Priorität. Doch der User Lifecycle bleibt ein Engpass. Unternehmen wollen immer effizienter arbeiten, indem sie ihre Dienstleistungen verbessern, Einsparungen erzielen und ihre Wettbewerbsfähigkeit steigern. Die automatisierte Pflege der Mitarbeiter-Accounts und die automatisierte Bereitstellung eines schnellen und korrekten Zugangs zu den Systemen würden die IT-Verwaltungsprozesse optimieren.	**Vollständige IDaaS-Lösungen beinhalten nun auch User Account Provisioning.** Organisationen möchten Mitarbeiter in einem Kernregistrierungssystem, wie z.B. das HR-System, verwalten, aus dem heraus alle Änderungen gesteuert werden. Das IDaaS-System erkennt die Änderungen (Dienstantritt und -austritt, Abteilungs- oder Namensänderungen usw.) und überträgt sie automatisch aus dem HR-System auf Benutzerkonten, E-Mail-Adressen, Zugriffsrechte, Lizenzen, IT-Ressourcen (Laptop, Tablet, Telefon).

Trend	Folge
In der digitalen Welt von heute ist die richtige Verknüpfung von Mitarbeiter und seinen Daten entscheidend für den Erfolg des Unternehmens. Vor 5 Jahren hatte nicht jeder in der Organisation ein persönliches Benutzerkonto oder ein E-Mail-Postfach. Häufig wurden noch Gruppenkonten verwendet. Dies ist heute keine Option mehr. Mitarbeiter müssen zu jeder Zeit, mit jedem Gerät und von jedem Ort aus Zugang zu ihren benötigten Daten haben. Das schafft sowohl neue Risiken als auch Chancen.	**Zero Trust Security-Modelle, verankert im Identity Management, sind die Zukunft.** Ohne einen korrekten und schnellen Zugang sind Mitarbeiter unproduktiv, werden unzufrieden und erzeugen Druck in den beteiligten Abteilungen. Über IDaaS ist es möglich, alle notwendigen IT-Ressourcen schnell und zuverlässig zu verwalten. Dazu gehört auch die einfache und einmalige Anmeldung (SSO) mit einem Smartphone (2FA) auf sichere Art und Weise.
Die „Black Box" IAM-System ist untragbar geworden. Identity-Management-Systeme sind oft komplex zu implementieren und zu verwalten. Das System ist eine unzuverlässige Black Box und es gibt immer mehr kritische Fragen zu den hohen Kosten, die mit dem IAM-System verbunden sind. Es gibt nur wenige Berater, und die sind teuer und kaum verfügbar.	**Unternehmen benötigen von Experten unterstützte, aktiv entwickelte IDaaS-Lösungen.** Moderne Software ermöglicht eine schnelle Anpassung an Veränderungen im Markt und in der Organisation. Entwicklungsteams gehen schneller auf Funktionswünsche der Kunden ein. Experten-Support wird intern bereitgestellt, mit transparenten und vorhersehbaren Kostenstrukturen.

Mit HelloID Identity Management von Tools4ever sind Sie auf diese wichtigen Entwicklungen vorbereitet.

Tools4ever bietet Ihnen Identity as a Service (IDaaS), eine vollwertige native Cloud-Lösung. HelloID automatisiert Ihren gesamten Identity Lifecycle und Ihre Benutzer erhalten einen benutzerfreundlichen und sicheren Zugriff auf Ihre IT-Dienste. Sie müssen nicht in Ihre eigene Infrastruktur mit Hardware, Datenspeicher und Software investieren.

Die Installation und Konfiguration erfolgen in wenigen Stunden und Tools4ever, ein Implementierungspartner oder Ihre eigene Organisation kümmert sich um die Verwaltung. Sie sparen Geld und Administrationsaufwand, jedoch nicht auf Kosten von Kontrolle und Sicherheit. Kunden von Tools4ever erhalten häufig Komplimente von IT-Auditoren, was die Einrichtung und den Betrieb von HelloID betrifft. Die Software läuft in einer vollständig abgesicherten Azure-Umgebung, die alle sechs Monate umfassend von Deloitte Risk Services überprüft wird. Die gesamte Lösung erfüllt die strengsten Sicherheitsanforderungen.

HelloID zwingt Sie nicht zu einem ‚Big Bang' mit viel Druck auf die Organisation und großen Risiken. HelloID ist in Module aufgeteilt und der Roll-Out kann in Phasen durchgeführt werden. Als Organisation können Sie frei wählen, mit welchen Modulen Sie beginnen und welche Funktionen Sie später aktivieren möchten. Es ist auch problemlos möglich, Funktionen wieder abzuschalten.

HelloID umfasst die folgenden Module:

1. Das Modul **Provisioning** bietet eine automatisierte Erstellung, Verwaltung und schließlich Löschung von Benutzerkonten auf Grundlage der Daten aus Ihrem HR-System. Das Provisioning verwaltet auch automatisch die damit verbundenen Rechte und weiteren Funktionen, abhängig von der Rolle und dem weiteren Kontext einer Person. Wenn sich die Rolle einer Person ändert, werden die Rechte automatisch entsprechend angepasst. Und wenn jemand die Organisation verlässt, kann das Benutzerkonto automatisch deaktiviert und gelöscht werden.

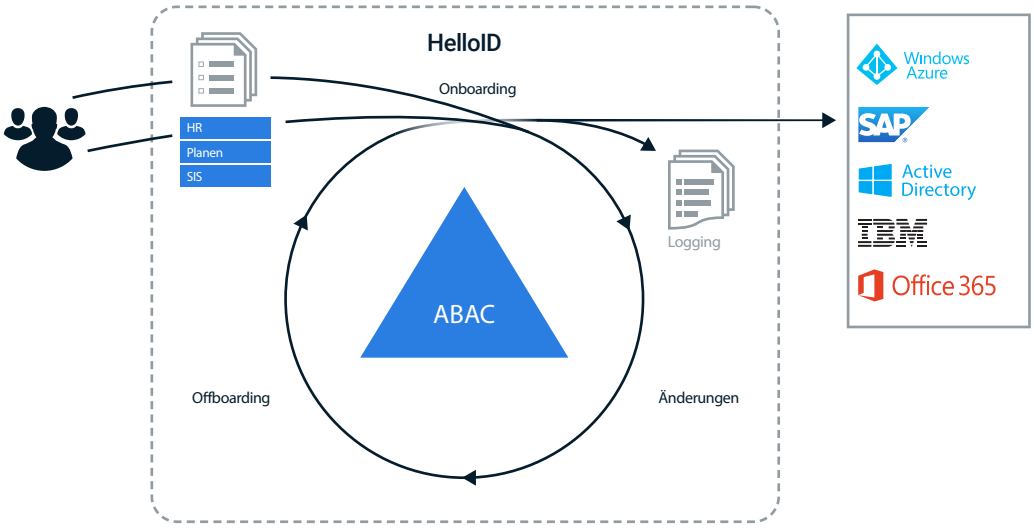
2. Das Modul **Service Automatio**n schließt nahtlos an das Pro¬visioning an. Neben dem automatisierten Provisioning aus dem HR-System gibt es immer wieder individuelle Service-Anfragen: Jemand benötigt vorübergehend bestimmte Software für ein Projekt oder Rechte an bestimmten Dateien. Hier kommt Service Automation ins Spiel. Mitarbeiter und Vorgesetzte haben Zugang zu einem Service-Portal mit allen IT-Produkten (Accounts, Berechtigungen, Software usw.), die (vorübergehend) angefordert werden können. Änderungen werden direkt im Netzwerk durchgeführt, ohne dass manuelle Änderungen durch die IT-Mitarbeiter nötig sind.

3. Das Modul **Access Management** dient zur sicheren und benutzerfreundlichen Verwaltung des Mitarbeiterzugangs für die unterschiedlichsten Anwendungen und Informationen. Benutzer können sich über einen Login mit Benutzernamen, Passwort und 2. Faktor am Portal authentifizieren. Nach dem Zugriff bietet HelloID ein benutzerfreundliches Dashboard, in dem Benutzer ihre Anwendungen einfach öffnen können. Dank der umfangreichen Single-Sign-On-Funktionalität genügt ein Klick.

Provisioning

Als Organisation müssen Sie zahlreiche Benutzerkonten verwalten: Festangestellte, Zeitarbeiter und oft auch Branchenpartner und Kunden. All diese Konten müssen erstellt, aktiviert, aktualisiert, deaktiviert und kontinuierlich gepflegt werden. Zusätzlich zu einem Hauptkonto (typischerweise Active Directory) benötigt jeder Benutzer Konten in anderen Zielsystemen. Rechte, Anwendungen und andere Ressourcen, müssen dann in allen Systemen verwaltet werden. HelloID Provisioning übernimmt die systemübergreifende und vollautomatische Erstellung, Änderung und Löschung von Konten. Damit automatisieren Sie den Onboarding-, Change- und Offboarding-Prozess, ihr gesamtes ‚Identity Lifecycle Management'.

Mit dem automatisierten Provisioning steigern Sie die Produktivität Ihrer Mitarbeiter, können Kosten für Routinearbeiten und teure Lizenzen einsparen und verbessern Ihre IT-Sicherheit.



Dank HelloID verfügt ein neuer Mitarbeiter am ersten Arbeitstag über ein Benutzerkonto mit entsprechenden Zugriffsrechten, die notwendige Software und weitere Zugänge. Wenn ein Mitarbeiter später an einen anderen Arbeitsplatz und/oder in eine andere Abteilung wechselt, stellt der HelloID-Änderungsprozess sicher, dass seine Rechte und Lizenzen automatisch angepasst werden. Und wenn ein Mitarbeiter aus dem Unternehmen ausscheidet? Dann kann die sofortige Sperrung des gesamten Kontos in HelloID veranlasst werden. Folgeaktionen wie das Einrichten einer Mailweiterleitung oder das Löschen von Mailbox- und Home-Directory-Daten, die erst Wochen oder Monate später durchgeführt werden müssen, können im Anschluss eingerichtet werden. Aufgaben die früher im Nachhinein per Hand durchgeführt wurden, werden jetzt automatisch von HelloID erledigt. Außerdem ist es möglich, Vorgänge einzuleiten, bevor der Mitarbeiter das Unternehmen verlässt. So kann beispielsweise der Vorgesetzte darüber informiert werden, dass bestimmte Geräte wie Laptop, Telefon usw. zurückgegeben werden müssen.

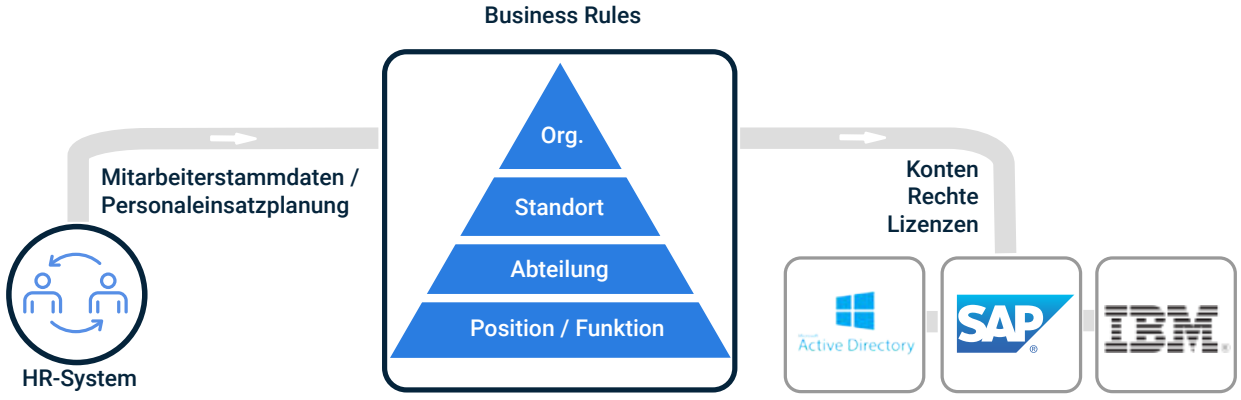
Das Provisioning macht die Verwaltung von Benutzerkonten einfacher, schneller und sicherer. Für HR- und IT-Teams ist die Benutzerverwaltung nicht länger eine manuelle, komplexe und zeitintensive Aufgabe. Zudem werden die Mitarbeiter produk¬tiver, weil ihnen immer sofort die richtigen Zugänge zur Verfügung stehen.

Das automatische Provisioning ist nicht nur komfortabel und effizient, sondern stellt auch ein leistungsstarkes zusätzliches Sicherheitstool dar. In vielen Unternehmen häufen Arbeitnehmer allmählich – auch unbeabsichtigt – immer mehr Rechte und Zugänge an. Es gibt oft kein automatisches Verfahren, um Rechte zurückzunehmen, wenn jemand sie nicht mehr benötigt. Häufig kommt es vor, dass ehemalige Mitarbeiter noch Zugang zu den Systemen haben, mit allen damit verbundenen Risiken. Das automatische Provisioning stellt sicher, dass Personen immer nur die Rechte haben, die für ihre Rolle notwendig sind. Wenn eine Änderung in der Funktion oder Abteilung eintritt, werden Rechte und Lizenzen entzogen, optional mit einer Übergangsfrist.

Diese automatische Rücknahme von Rechten und Zugängen bietet auch einen unmittelbaren Kostenvorteil. Vielen Unternehmen entstehen unnötige Kosten für teure Lizenzen und Zugänge, die nicht mehr genutzt, aber monatlich in Rechnung gestellt werden. Mit HelloID können Sie diese Kosten viel besser in den Griff bekommen.

Attribute Based Access Control (ABAC)

Ein zentrales Element des Provisioning ist Attribute Based Access Control. Mit ABAC wird sichergestellt, dass die Mitarbeiter Zugang zu den richtigen IT-Ressourcen haben, die sie für ihre Arbeit benötigen. Je nach der Rolle, die jemand in der Organisation innehat und der damit verbundenen Arbeit, benötigt ein Mitarbeiter also bestimmte Komponenten aus der IT. Diese Umsetzung erfolgt über ABAC. Auf Grundlage der Kombination von zum Beispiel Funktion und Abteilung werden Konten, Rechte, Lizenzen und IT-Ressourcen (Laptop, Arbeitsplatz, Telefon usw.) bereitgestellt.



Aufgrund der Verschärfung von Gesetzen und Vorschriften (wie BSI, DSGVO, FISMA, HIPAA, SOX, NEN7510) hat ABAC in den letzten Jahren zunehmend an Bedeutung gewonnen. Früher war ABAC hauptsächlich eine Domäne von Finanzinstitutionen und großen internationalen Unternehmen. Heutzutage wird ABAC auch in Gesundheitseinrichtungen, mittelständischen Unternehmen (300-5000 Mitarbeiter) und anderen kommerziellen Organisationen benötigt.

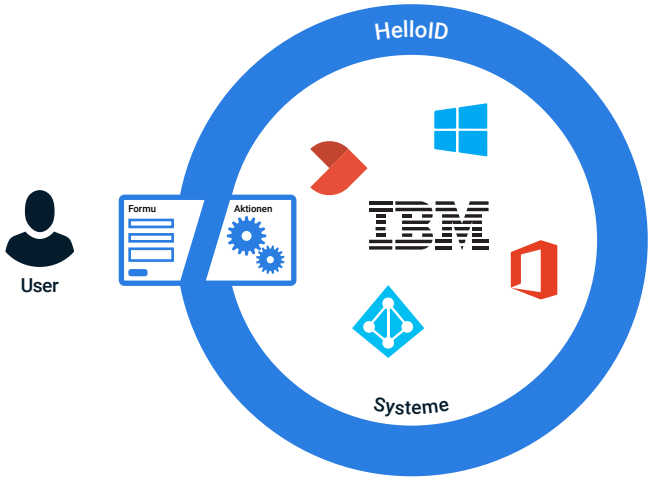
Als Organisation möchten Sie die volle Kontrolle darüber haben, wer zu welchen Systemen Zugang hat. Sie erwarten ein klares Zusammenspiel von Benutzerfreundlichkeit und Betriebssicherheit. Mit zu wenigen und zu spät bereitgestellten Rechten behindern Sie Ihre Mitarbeiter in ihrer Arbeit. Mit zu vielen Rechten geht die Organisation große Risiken ein. Viele Unternehmen stoßen in dieser Hinsicht an ihre Grenzen. Die manuelle Zuordnung und Verwaltung der Rechtestruktur ist äußerst komplex, zeitaufwändig und fehleranfällig. Das schnelle Erstellen von Benutzern auf der Basis von Benutzer kopieren – „Stefanie wird die gleiche Arbeit machen wie Annette" – ist wiederum zu einfach. Mit der ABAC-Funktionalität können Sie diese Verwaltung auf praktische und einfache Weise auf ein ausgereiftes Niveau bringen.

Innerhalb von HelloID implementieren wir ABAC über unsere Business-Roles-Funktionalität. Business Roles bieten die Möglichkeit, die Rechtestruktur phasenweise aufzubauen. Sie bringen Organisationen nach und nach vom bisherigen Stand auf eine professionelle Plattform, die es ihnen ermöglicht, Rechte kontrolliert zu verwalten, ohne sofort alle Rollen und Rechte abbilden zu müssen. Das folgende Diagramm bietet einen schematischen Überblick über den Ansatz von Business Roles in HelloID. Auf der Grundlage von Verträgen und Personaleinsatzplanung wird per Mitarbeiterebene (Organisation, Abteilung, Funktion und Rolle) festgelegt, welcher Zugang (Konten, Rechte und Lizenzen) im Netzwerk erforderlich ist, um die Arbeit auszuführen.

Service Automation

Der Provisioning-Prozess automatisiert praktisch alle IT-bezogenen Änderungen. Es gibt jedoch Ausnahmen, da nicht alles im HR-System registriert ist. Denken Sie an einen Mitarbeiter, der vorübergehend die Arbeit eines kranken Kollegen übernimmt, oder an einen Mitarbeiter, der für ein bestimmtes Projekt eingesetzt oder an eine andere Abteilung ausgeliehen wird. Zur Durchführung dieser zusätzlichen Aufgaben benötigt der Mitarbeiter z. B. zusätzliche (aber oft temporäre) Zugriffsrechte auf Dateien, zusätzliche Rechte zur Durchführung von Aktionen in SAP, eine MS-Projektlizenz, Mitgliedschaft in einer Verteilerliste, Mitgliedsstatus einer MS-Teams-Seite usw.

In vielen Unternehmen werden diese Arten von Änderungen manuell vom IT-Helpdesk bearbeitet, was teuer und zeitaufwändig ist. Service Automation automatisiert daher auch diese temporären Änderungen. Über einen Self Service Webshop können Mitarbeiter ohne IT-Kenntnisse oder Domain-Administrator-Rechte sicher selbst Änderungen im Netzwerk vornehmen. Dies erfolgt über eine delegierte „Shell“ rund um das Netzwerk und alle Änderungen werden mittels definierter Szenarien über die HelloID-Engine im Netzwerk ausgeführt. Und das nach genau definierten Schritten, immer auf die gleiche Art und Weise, mit einem vollständigen Audit-Protokoll.



Das Modul Service Automation bietet Ihnen folgende Vorteile:

- Self-Service: Soweit von der IT freigegeben, kann jeder auf sichere und kontrollierte Weise Änderungen im Netzwerk vornehmen, eventuell auch über Genehmigungsworkflows. Der Helpdesk muss nicht mehr aktiv werden und stellt keinen Verzögerungsfaktor dar. Vorgesetzte haben einen unmittelbaren Einblick, welche Zugänge ihre Mitarbeiter haben und können diese sofort anpassen.
- Es ist direkt ersichtlich, wer welche Lizenzen nutzt, ob zu viele Lizenzen verwendet werden und wie viele Lizenzen noch verfügbar sind. Vorgesetzte können leicht erkennen, wie der ‚IT-Fußabdruck‘ ihrer Abteilung aussieht.

- Änderungen unterliegen einer zeitlichen Begrenzung. Dies verhindert eine uner wünschte Anhäufung von Rechten und Lizenzen. Dieses Thema ist sicherlich ein Schwerpunktbereich für Wirtschaftsprüfer und die Akkumulation von Berechtigungen führt oft zu einer negativen Beurteilung.
- Modernes und professionelles Auftreten gegenüber der Organisation und den Mitarbeitern, die neu eingestellt werden.
- HelloID SA ist nahtlos in verschiedene ITSM-Plattformen (ServiceNow, TOPdesk) integriert. Dadurch ergeben sich für den Endanwender keine Änderungen und die Benutzerakzeptanz ist hoch, da nicht (wieder) ein neues Portal eingeführt wird.

Service Automation kann große organisatorische Auswirkungen haben. So erhalten Mitarbeiter und Vorgesetzte eine andere und wichtigere Rolle bei der Vergabe von IT-Zugängen. Um die Implementierung so einfach wie möglich zu gestalten, kann Service Automation Schritt für Schritt eingeführt werden. Diese Schritte werden im Folgenden beschrieben:

Delegation an den Service Desk

Im ersten Schritt werden Arbeitsaufgaben von Systemspezialisten (wie z. B. Second- und Third-Level-Systemadministratoren oder funktionalen Anwendungsadministratoren) über delegierte Formulare an ungelernte/angelernte Service-Desk-Mitarbeiter delegiert. Der Clou: Es werden keine Admin-Rechte benötigt. Änderungen werden immer auf die gleiche Weise implemen¬tiert, es sind keine IT- oder Anwendungskenntnisse erforderlich, um die Änderung durchzuführen, und jede Änderung wird protokolliert. Service Automation ist eine „Shell“ um das Netzwerk, jede Änderung wird über SA kontrolliert und gesteuert.

Delegation an den Vorgesetzten

Die Delegation an den Vorgesetzten ist der nächste Schritt. Aus technischer Sicht ist dies ein einfacher Schritt, da die Formulare und Vorgänge für die Mitarbeiter des Service-Desks bereits definiert sind. Aus Sicht der Organisation ist es ein großer Schritt, da mehr Mitarbeiter direkt mit HelloID in Berührung kommen. Nach diesem Schritt haben Vorgesetzte sofort Einblick, welche Zugriffsrechte ihre Mitarbeiter haben und welche Lizenzen sie nutzen. Der Vorgesetzte kann dann sofort selbst Änderungen vornehmen oder eigenständig Berechtigungen für einen Mitarbeiter hinzufügen oder entfernen. Es gibt keinen umständlichen Prozess mehr mit Service-Tickets und -Mitarbeitern, um diese Vorgänge auszuführen.

Delegation an den Endanwender

Der letzte Self-Service-Schritt ist die Delegation an den Endanwender. Eine wichtige Voraussetzung dafür ist die Integration in bestehende Self-Service-Portale, wie z. B. TOPdesk oder ServiceNow usw. Hinzu kommt eine Genehmigungsstufe, in der beispielsweise der Vorgesetzte einen Antrag beurteilt, bevor er implementiert wird. Diese Kontrolle verhindert, dass Endanwender Zugänge anfordern, die für die Erfüllung ihrer Aufgaben nicht notwendig sind. Die Kontrolle ist für einen Vorgesetzten oder Lizenzverwalter viel einfacher als für einen IT-Mitarbeiter. Nach der Genehmigung stellt das Modul Service Automation sicher, dass die Änderungen automatisch im Netzwerk implementiert werden.

Access Management

Das Modul Access Management bietet Mitarbeitern, Partnern und Kunden einen einheitlichen, benutzerfreundlichen Zugriff auf Cloud-Anwendungen. Die Authentifizierung erfolgt über einen Benutzernamen mit Passwort und einen zweiten Faktor (Multi-Faktor-Authentifizierung) Ihrer Wahl.

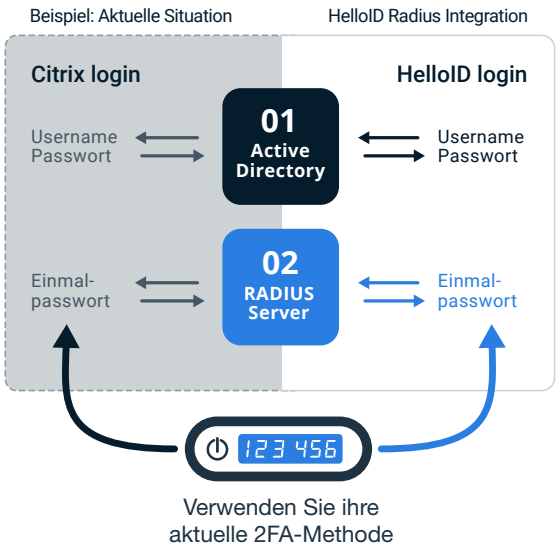
Die Benutzer können über ihren Computer, ihr Tablet oder ihr Smartphone auf ein benutzerfreundliches Dashboard zugreifen. Jede einzelne Cloud-Anwendung ist anhand eines wiedererkennbaren Symbols mit einem Klick aufrufbar. Dabei muss sich der Endanwender nur einmal pro Sitzung anmelden. HelloID unterstützt alle gängigen Single-Sign-On-Protokolle, um den Benutzer pro Cloud-Anwendung automatisch zu authentifizieren.

Der Benutzer durchläuft somit drei Teile des HelloID Access Managements:

1. Der Mitarbeiter muss nachweisen, dass er die Person ist, die er vorgibt zu sein (Authentifizierung)
2. Der Benutzer erhält einen Überblick über die Anwendungen, für die er Zugriffsrechte besitzt (Dashboard)
3. Der Benutzer wählt eine Anwendung aus und gelangt direkt in die Zielanwendung, ohne sich erneut anmelden zu müssen (Single Sign-On). Diese drei Bestandteile von HelloID Access Management werden im Folgenden näher erläutert.

Authentifizierung

In vielen Fällen melden sich die Benutzer via Active Directory an HelloID an. HelloID unterstützt auch andere Identity Provider wie Azure, Google, SAML, Salesforce usw. Alternativ kann das lokale HelloID-Directory verwendet werden, beispielsweise wenn Kunden oder Patienten verwaltet werden sollen, ohne zuvor für diese Benutzer Accounts im Active Directory oder einem anderen Identity Provider anzulegen. HelloID bietet eine umfassende 2FA-Technologie und ist hinsichtlich der Kosten äußerst wettbewerbsfähig (z. B. im Vergleich zu Azure P1).



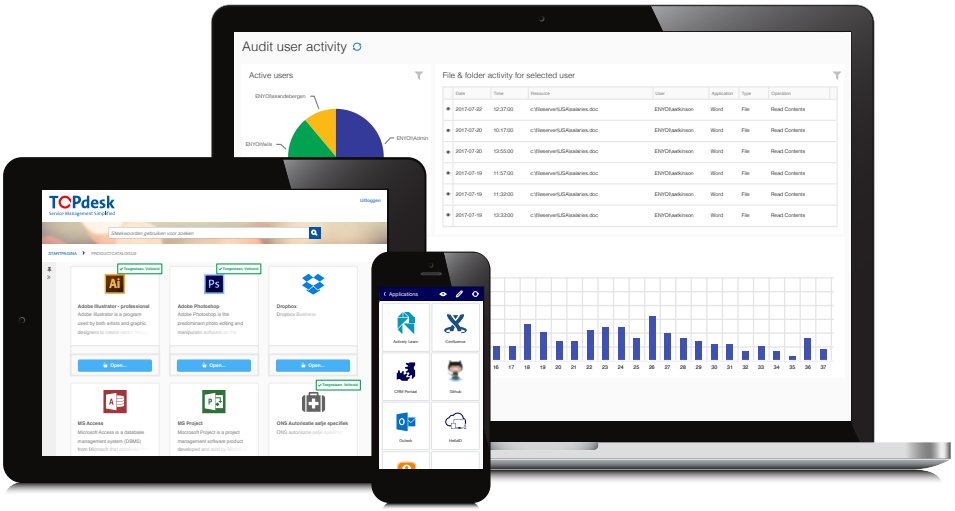
Neben Software (Push-to-Verify-App) oder Hardware-Token und SMS werden als zweiter Faktor verschiedene OTPs (Einmal-Passwörter) unterstützt. Abhängig von den Anforderungen des Unternehmens bietet HelloID zahlreiche Integrationsmöglichkeiten, einschließlich Radius-Integration.

Dashboard

Nach erfolgreicher Anmeldung erhalten die Endanwender Zugang zu einem Online-Dashboard. Über Icons hat der Benutzer direkten Zugriff auf die verknüpften Cloud-Anwendungen. Bestehende On-Premise Anwendungen bleiben über z. B. Citrix erreichbar. Das Citrix-Icon befindet sich selbstverständlich auf dem Dashboard und ist somit auch mit der integrierten 2FA und den Acces Policies von HelloID abgesichert.

Welche Anwendungen angezeigt werden, hängt von den Rechten des Benutzers innerhalb des Unternehmens ab. So lassen sich Gruppen von Mitarbeitern auf Basis von Funktion, Standort usw. erstellen. Anschließend werden die Anwendungen auf Gruppenbasis autorisiert. So haben Sie die Kontrolle darüber, wer Zugriff auf welche Anwendung erhält. Durch die Integration mit beispielsweise dem Active Directory kann die Platzierung von Benutzern in Gruppen mit denen im AD synchronisiert werden. Dies stellt für Administratoren eine enorme Arbeitserleichterung dar. So kann über die AD-Gruppenzugehörigkeit festgelegt werden, welche Cloud-Anwendungen ein Mitarbeiter nutzen kann und ob dies zusätzliche 2FA-Ebene erfordert.

Nicht zuletzt lässt sich das Layout des Dashboards komplett individuell konfigurieren. Die Standardansicht kann mit eigenen CSS-Stylesheets oder integrierten Links angepasst werden. Über die Enduser-API lässt sich das Dashboard in Social-Intranet-Anwendungen wie TripTic, Embrace, a&m impact, Workplace365, Motivo, Google Sites oder SharePoint Online einbinden.



Single Sign-On (SSO)

Nach der Authentifizierung im HelloID-Dashboard kann der Anwender automatisch bei anderen Anwendungen angemeldet werden. HelloID speichert die Anmeldedaten des Benutzers für jede Anwendung und leitet sie automatisch über das entsprechende SSO-Protokoll weiter, wenn der Benutzer eine Anwendung startet. Der User muss sich nicht erneut anmelden, es sei denn, es wurden zusätzliche Anforderungen festgelegt (z. B. eine zweite 2FA-Ebene).
Um diesen Single Sign-On (SSO) für die verschiedenen Anwendungen zu ermöglichen, unterstützt HelloID alle bestehenden SSO-Protokolle wie OpenIDconnect, SAML, HTTP(S) Post, Basic Authentication usw.

Über Tools4ever

Tools4ever ist ein europäisches Software-Unternehmen. Wir entwickeln innovative und standardisierte IDaaS-Lösungen. Heutzutage wird Identity as a Service immer komplexer, weshalb wir es uns zur Aufgabe gemacht haben, IDaaS-Lösungen zu entwickeln und zu liefern, die einfach zu implementieren und zu verwalten sind. Von 2013 bis 2020 haben wir maximale Investitionen getätigt, um dieses Ziel zu erreichen. HelloID wurde von Grund auf mit den modernsten Software-Techniken entwickelt. Das erste Release von HelloID wurde Anfang 2020 mit großer Unterstützung aufgenommen. HelloID ist ein hervorragendes Produkt, das unsere Anwender sehr gerne nutzen. Wir haben uns verpflichtet, ausgezeichnete Leistungen zu einer fairen Vergütung zu erbringen und kontinuierlich in die Weiterentwicklung von HelloID zu investieren.

TOOLS4EVER
IDENTITY GOVERNANCE & ADMINISTRATION

Tools4ever Informatik GmbH

Adresse Hauptstraße 145-147
51465 Bergisch Gladbach
Deutschland

Telefon +49 2202 2859 0
Website www.tool4ever.de

Info info@tools4ever.de
Sales sales@tools4ever.de