PEOPLE.ACCESS.DATA.

20 JAHRE
TOOLS4EVER ANNO 1999

TOOLS4EVER.MAGAZIN
NEWSLETTER

TOP-THEMA:

DATENSICHERES ON- UND OFFBOARDING VON MITARBEITERN

TOOLS4EVER
IDENTITY GOVERNANCE & ADMINISTRATION

„Schluss mit den analogen Laufzetteln und dem unkontrollierten Zugriff auf Benutzerkonten und Daten: Einfach datensicheres On- und Offboarding von Mitarbeitern.“

Foto: r.classen/shutterstock.com

EIN PERFEKTER ERSTER ARBEITSTAG

1

SO WIRD ONBOARDING ZUM ERFOLG!

EUPHORIE, VORFREUDE UND ETWAS NERVOSITÄT: DER ERSTE TAG IM NEUEN UNTERNEHMEN IST IMMER AUFREGEND. DIE KOLLEGEN BEGRÜßEN, DEN SCHREIBTISCH EINRICHTEN UND DANN DAS ERSTE MAL DEN NEUEN RECHNER HOCHFAHREN, EINLOGGEN UND ... ALLES LÄUFT!

DER ERSTE EINDRUCK ZÄHLT

Gerade zu Beginn eines neuen Arbeitsverhältnisses möchten Mitarbeiter mit viel Elan die neuen Herausforderungen angehen.

Umso frustrierender ist es, wenn der Motivation bereits am ersten Arbeitstag ein Dämpfer verpasst wird. Anstatt sich an die Arbeit zu machen, heißt es allzu oft auf IT-Ressourcen warten, mit dem Laufzettel durch das Unternehmen eilen oder sich die notwendigen Arbeitsmittel selbst besorgen.

Unternehmen stehen heute im Wettbewerb um die besten Fachkräfte und geben dabei für das sogenannte Employer Branding viel Geld aus: Sie tunen ihre Anzeigen, geben sich modern auf Karrieremessen, ja sie frischen sogar ihre Arbeitsweisen auf mit Gleitzeit, flexibleren Urlaubszeiten und mit unzähligen Work-Life-Balance-Angeboten. Doch den ersten Arbeitstag haben viele nicht im Blick. Das mit großer Mühe aufgebaute Bild wird gleich zerstört – der neue Mitarbeiter ist frustriert.

Unternehmen verpassen oft beim sogenannten Onboarding neuer Mitarbeiter die Chance, sich positiv hervorzutun und den ersten Arbeitstag zum perfekten Erlebnis zu machen. Der Arbeitsplatz sollte zum Start richtig eingerichtet sein. Dafür sind ein Schreibtisch und der passende Stuhl ebenso wichtig wie die persönlichen Zugänge zu den Systemen. Und idealerweise läuft die Vergabe von Benutzerrechten automatisiert ab.

Häufig ziehen sich die mangelhaften Abläufe des Onboardings über die gesamte Dauer der Anstellung des Mitarbeiters durch bis zum Offboarding: Nach ein paar Jahren im Unternehmen wissen die Verantwortlichen meist nicht mehr, welche Schlüssel die Mitarbeiter ausgehändigt bekommen haben. Ebenso unklar ist, welche Zugriffsrechte ein Mitarbeiter hat, wenn identitätsbezogene Arbeiten schrittweise, undokumentiert und manuell ablaufen. So fällt es entsprechend schwer, den Mitarbeiter sofort nach Verlassen von allen Systemen und Berechtigungen abzukoppeln – vor Ort (On Prem) und in der Cloud.

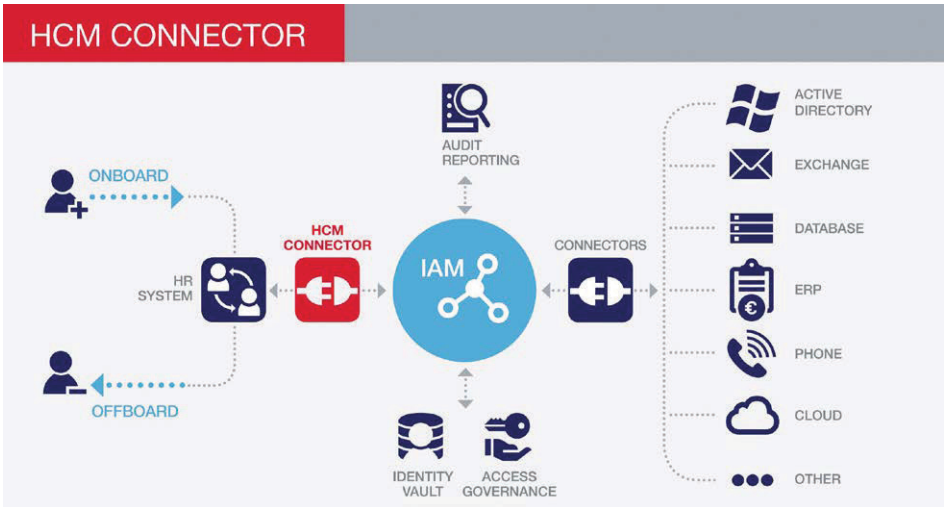
Es lohnt sich also, die On- und Offboarding-Prozesse im eigenen Unternehmen einmal genau unter die Lupe zu nehmen: In vielen Fällen hilft ein professionelles Identity- und Accessmanagement, um eventuelle Datenschutzlücken zu schließen, Sicherheitsrisiken zu minimieren und gleichzeitig den ersten beziehungsweise letzten Eindruck vom Unternehmen zu verbessern.

2 IDENTITÄTS- UND ACCESSMANAGEMENT

IDENTITÄTS- UND ACCESSMANAGEMENT (IAM) MACHT DAS ON- UND OFFBOARDING VON MITARBEITERN EINFACH DATENSICHER – DIE IT WIRD ENTLASTET.

Tools4ever realisiert Identity- und Accessmanagement-Lösungen mit integrierter Verbindung zur Personalabteilung. Dabei sorgt ein so genannter Human Capital Management (HCM) Connector für die Verbindung zwischen Personalsystem und der Benutzerverwaltung im Netzwerk. Die Personalabteilung pflegt die Mitarbeiterdaten wie gewohnt in SAP HCM, P&I Loga oder Sage. Änderungen werden automatisch von IAM im Netzwerk erkannt und verarbeitet. Die Eingabe und Pflege von Zugriffsrechten beziehungsweise Daten verlagert sich in die Organisation und die IT wird entlastet. Dabei behält die Organisation die Kontrolle über Mitarbeiterdaten und kann selbst überblicken, welcher Mitarbeiter wann Zugriff auf welche Daten und Systeme hat. Das An-, Um- und Abmelden von Mitarbeitern wird einfacher, schneller, direkter, sicherer und DSGVO-konform.

Tools4ever entwickelt **Komplett-Lösungen im Identity- und Accessmanagement (IAM)** und implementiert individuelle Software-Konzepte weltweit. Damit stärkt Tools4ever die Compliance und Sicherheit in mittleren und großen Organisationen. Gerade die europaweite Einführung der neuen Datenschutzgrundverordnung (DSGVO) sorgt für eine steigende Nachfrage nach effektiven, transparenten und sicheren Lösungen im Zugriffsmanagement. Automatisierung und Self-Service liegen dabei im Trend: Vor allem beim On- und Offboarding von Mitarbeitern sind neue Ideen gefragt, denn datensichere IAM-Lösungen spielen eine zunehmend wichtige Rolle. „Es sind immer häufiger die Personal- oder die Sicherheitsbeauftragten, die nach Unterstützung für eine sichere und direkte An-, Um- und Abmeldung von Mitarbeitern fragen. Die Personalleiter wollen den ersten Tag im Unternehmen zum ‚tollen' Erlebnis für Mitarbeiter machen – mit sofortigem Zugang zu E-Mail, Internet und Daten. Nach dem Ausscheiden eines Mitarbeiters will die Organisation dann alle Zugänge wieder kontrolliert und einfach sperren können", weiß Jan Pieter Giele. Seit 2004 leitet er die Geschäfte von Tools4ever in Deutschland. Giele weiß, dass gerade die Frage nach Ex-Mitarbeitern, die noch Zugriff auf Systeme oder Daten haben könnten, vielen Führungskräften Kopfschmerzen bereitet.



Der Human-Capital Management Connecter (HCM) sorgt für die Verbindung zwischen Personalsystem und der Benutzerverwaltung im Netzwerk (Quelle: Tools4ever).

3 EIN TOOLS4EVER GUIDE

EINFACHES UND DATENSICHERES ON– UND OFFBOARDING IN FÜNF SCHRITTEN.

Das Identitäts- und Accessmanagement-System von Tools4ever ermöglicht dank innovativer Softwarelösungen ein datensicheres On- und Offboarding. Eine einfache Anwendung und Implementierung sind dabei von größter Bedeutung, um Prozesse effizienter zu gestalten. IAM von Tools4ever stellt anhand von Automatisierung mit der Möglichkeit zum Self-Service professionelles On- und Offboarding sicher. **Hierzu bedarf es nur fünf einfacher Schritte:**

1 SCHRITT 1: AUTOMATISCHES ANLEGEN UND BERECHTIGEN

Das IAM-System gewinnt über Schnittstellen zur Personalsoftware wie SAP HCM, P&I Loga oder Sage die relevanten Datensätze und legt auf dieser Grundlage automatisch Benutzerkonten an. Basierend auf definierten Attributen und Rollen weist das IAM den Benutzern spezifische Zugriffsrechte – sogenannte Birthrights – zu. Der Zugang auf Informationen oder Systeme, die der Benutzer für seine Arbeit nicht benötigt, bleibt gesperrt. Das Anlegen und Berechtigen von Benutzerkonten läuft also automatisch und ohne weiteres Zutun ab.

2 SCHRITT 2: AUTOMATISIERTE VERKNÜPFUNG DER BENUTZER MIT BERECHTIGUNGEN

Die Verknüpfung der zuvor angelegten Benutzerkonten mit den jeweiligen Berechtigungen erfolgt ebenfalls automatisch. Anpassungen in aufwendiger, manueller Kleinarbeit durch Administratoren oder Help-Desk-Manager sind nicht länger nötig. Weil derzeit immer mehr und komplexere Benutzerkonten auf immer mehr und komplexere Zielsysteme treffen, setzt Tools4ever auf automatisierte User-Lifecycle Management Prozesse (ULM). Auf diese Weise werden alle Zugriffsrechte digital kontrolliert und dokumentiert.

3 SCHRITT 3: VERWALTUNG VON BENUTZERRECHTEN

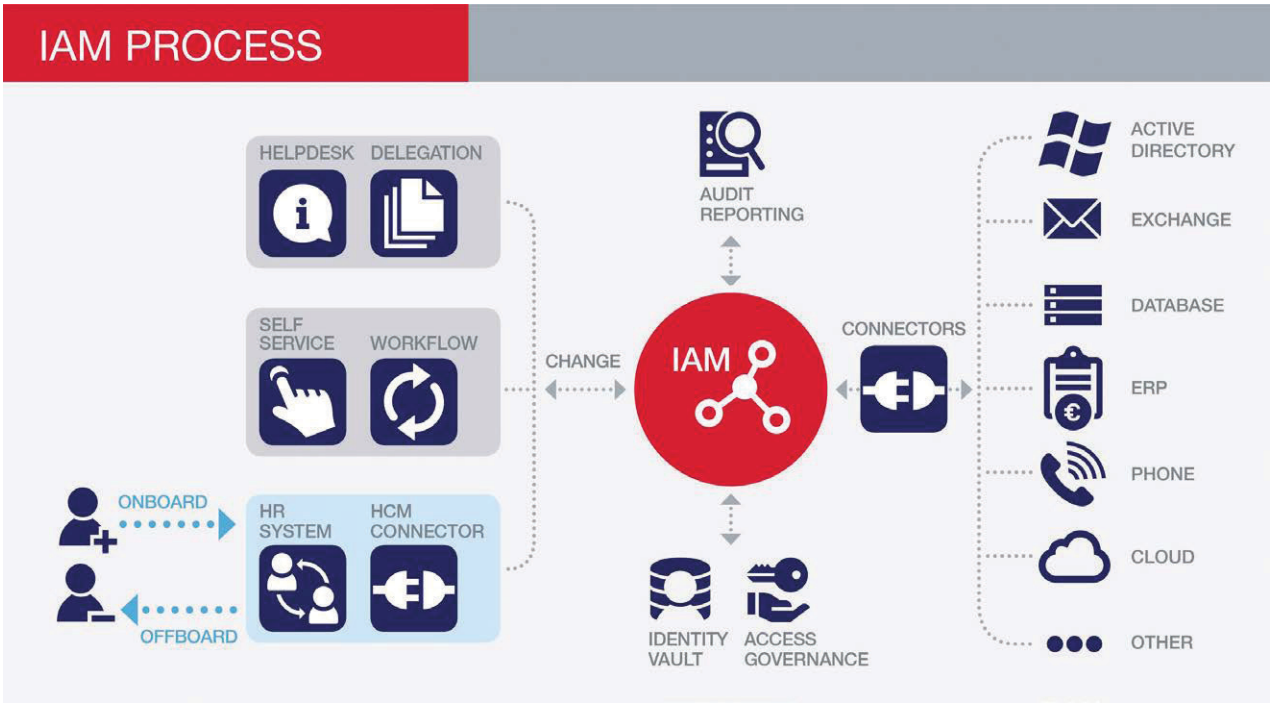
Die Verwaltung von Benutzerrechten – auch Access Governance genannt – ist so konzipiert, dass Mitarbeitern auch nur die Anwendungen zur Verfügung stehen, die sie benötigen. Mit Hilfe der Access Governance im IAM werden Zugriffsrechte nicht länger manuell und unkontrolliert vergeben. Spezielle Techniken und Prozesse von Tools4ever sorgen dafür, dass Benutzerrechte korrekt entsprechend der definierten Rolle vergeben werden. Abweichungen und Anomalien werden darüber hinaus überprüft und gemeldet.

4 SCHRITT 4: SPEZIFIZIERUNG DURCH DAS SELF-SERVICE TOOL

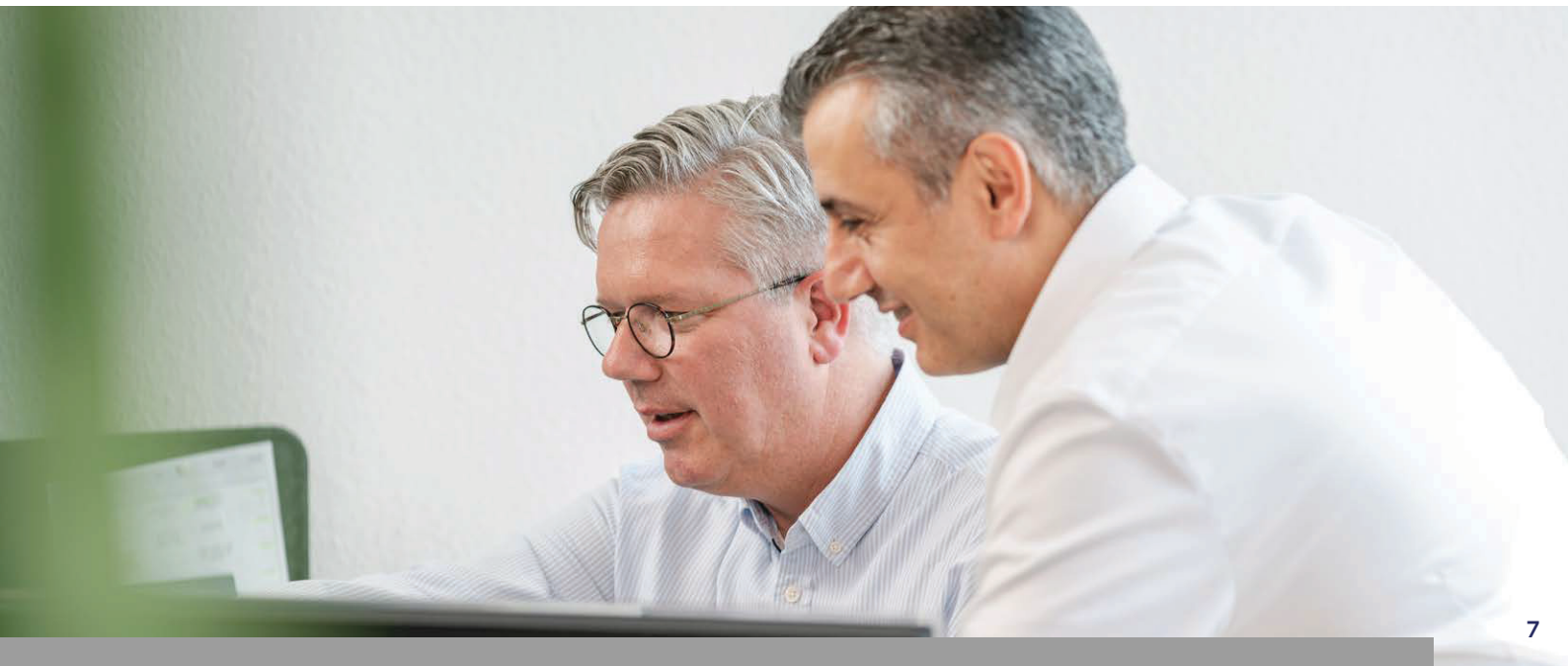
In den Schritten 1 bis 3 werden Identitäten mit ihren jeweiligen Zugriffsrechten automatisch – quasi auf Knopfdruck – erstellt. Sollten Benutzer zusätzlich zu ihrer vordefinierten Rolle Zugriffsrechte benötigen, können diese mit dem Self-Service Tool vergeben werden. Vorgesetzte sind so in der Lage, individuelle Berechtigungen zu vergeben oder Zugänge wieder zu sperren. Die Unterstützung durch Help-Desk-Manager, IT-Administratoren oder anderer Mitarbeiter wird dabei nicht benötigt: Die Organisation verwaltet auf diese Weise eigenständig den Zugriff auf spezielle Ordner, Anwendungen, Verteilerlisten oder E-Mail-Konten im Netzwerk. Dank des Self-Service Tools wird die IT maßgeblich entlastet – neue Kapazitäten werden geschaffen und gleichzeitig Geld und Zeit gespart.

5 SCHRITT 5: KONTROLLE UND ÜBERSICHT BEHALTEN

Aktualisierte Compliance-Richtlinien und neue gesetzliche Vorgaben wie etwa die DSGVO erfordern neue Lösungen in Sachen Datenschutz: Umso wichtiger ist es also, die eigenen Systeme vor dem Zugriff Unbefugter zu schützen. Damit einher geht die Notwendigkeit, nachweisen zu können, wer wo Zugriff hat. Neben IAM bietet die sogenannte ERAM Software speziell für das Filesystem transparente und korrekte Übersichten sowie einen Ansatz, die „gewachsene Berechtigungsstruktur“ im Filesystem zu bereinigen. Diese Dokumentation dient als Fundament für die Datensicherheit im Unternehmen.



Identity- und Accessmanagement machen die Arbeit transparenter, datensicherer und effizienter.



> Worst-Password-Studien sind erheiternd und erschreckend zugleich, da gehören „qwertz“ oder „123456“ tatsächlich zu den Ranglistenführern.“

4 „QWERTZ“

ONBOARDING–RISIKEN IM UNTERNEHMEN ÜBERWINDEN

Sie gehört zu den nervigsten Momenten, die während der Arbeit am Computer auftauchen: die gefürchtete Benachrichtigung „Password eingeben“. Dass wir uns ständig irgendwelche Passwörter merken müssen, ist das eine. Das andere ist, dass wir uns bei der Festlegung individueller Passwörter permanent an Regeln zur Bildung erinnern müssen. „Wie lang muss / darf das Wort sein?“ und „Wie viele Sonderzeichen und Zahlen braucht es?“.

Wir wollen am liebsten einen Schlüssel, der zu jedem Schloss passt. Daher machen wir es uns so leicht wie möglich. Der Mensch tendiert zur Einfachheit. Das Resultat sind oft unsichere Passwörter. „Worst-Password“-Studien sind erheiternd und erschreckend zugleich, da gehören „qwertz“ oder „123456“ tatsächlich zu den Ranglistenführern. Das ist bekannt.

Aber: Wissen wir auch, wo unsere Unternehmen am verwundbarsten sind, wenn es um die Vergabe und Vertei-lung von Passwörtern geht?

Stichwort Initialpasswort-Formel: Viele Unternehmen verwenden beim Erstellen neuer Konten eine simple Formel für die Standardkennwörter oder sogar das gleiche Standardpasswort für jedes einzelne neue Benutzerkonto. Nicht selten dürfen sich alle neuen Mitarbeiter mit dem Kennwort „neuermitarbeiter“ anmelden. Dass diese Praxis grob fahrlässig ist und Tür und Tor für Missbrauch mit Daten und Systemen öffnet, liegt auf der Hand. Dabei kann man noch froh sein, wenn diese Schwachstelle nur für Späße oder Streiche genutzt wird – und nicht, um dem Unternehmen oder Mitarbeitern zu schaden.

Stichwort Passwortübermittlung: Die Realität sieht oft so aus: Passwörter werden an die Teamleiter oder Vorgesetzten geschickt – und die sollen sie einfach an die neuen Mitarbeiter weitergeben. Oder es wird die private E-Mail-Adresse des neuen Mitarbeiters genutzt, um das Passwort zu zuschicken. Üblich ist auch ein Post-It-Zettel auf der Tastatur. Passwörter sind Geheimnisse und verlieren an Wert, je mehr Personen oder Wege an der Übermittlung beteiligt sind.

Stichwort verwaiste Konten: In vielen IT-Abteilungen gehört die massenhafte Erstellung von Konten für neue Benutzer zur täglichen Arbeit – für Saisonarbeiter oder Auszubildende, Praktikanten oder studentische Aushilfen. Wenn die Aushilfskraft das Unternehmen nach wenigen Wochen wieder verlässt oder die Stelle erst gar nicht angetreten hat, gibt es häufig keine Routinen oder Möglichkeiten zu überprüfen und zu überwachen, ob Konten überhaupt verwendet wurden. Verwaiste Benutzer-konten in der Organisation bilden ein enormes Sicherheitsrisiko – vor allem dann, wenn niemand weiß, dass sie existieren. Mit Hilfe von IAM-Lösungen in Kombination mit einem Passwort Self-Service Tool lassen sich diese Sicherheitsrisiken einfach und schnell beheben.

Sie gewährleisten, dass …

- **… neue Passwörter als zufällig generierte Zeichenketten entstehen;**
- **… Sicherheitslücken bei der Übertragung von Konten- und Anmeldeinformationen an neue Benutzer geschlossen werden;**
- **… die Übersicht und Kontrolle schon mit dem ersten Login**

5

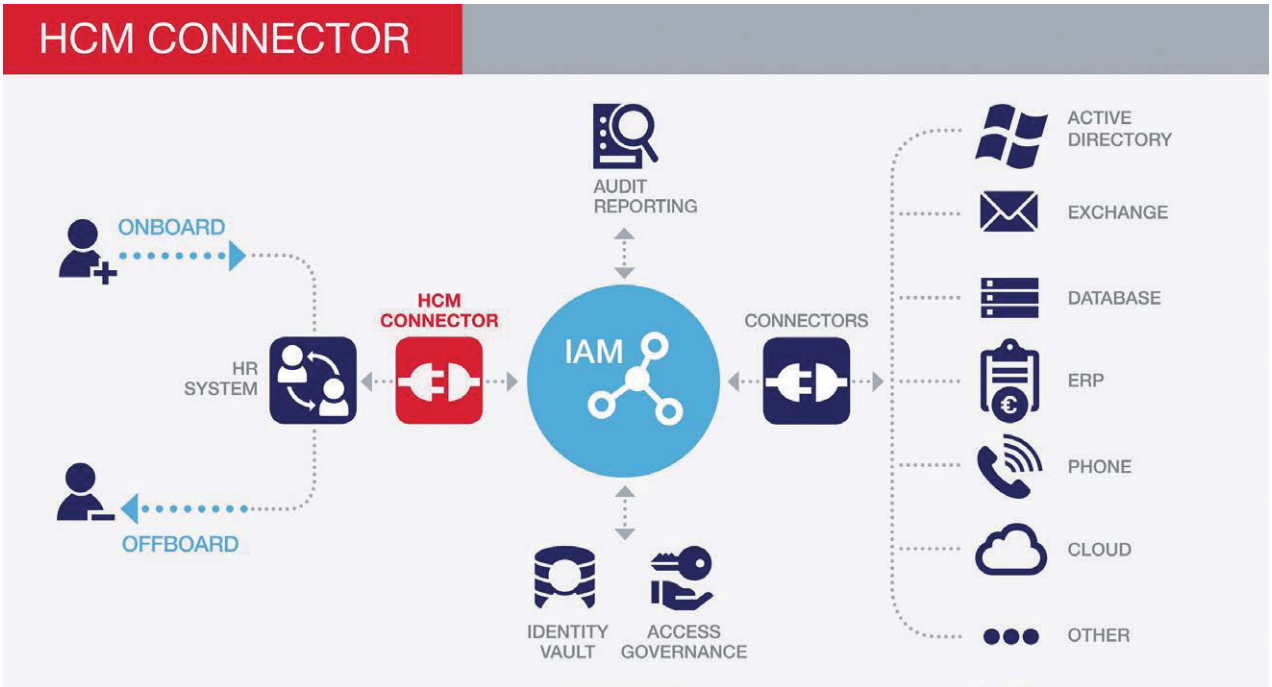
WENN DER EX NOCH ZUGANG HAT…

OFFBOARDING GEHT BEI IHNEN NICHT AUF KNOPFDRUCK?

On- und Offboarding-Prozesse können zu einem Alptraum für IT-Leiter und Management werden. Gerade das Offboarding erfordert die vollständige Entkopplung eines Mitarbeiters von allen Konten und Systemen – vor Ort (On-Prem) und in der Cloud. Nicht selten haben Ex-Mitarbeiter nach ihrem Ausscheiden (Offboarding) noch Zugänge zu den Räumen, aber vor allem zu den IT-Systemen, Datenbanken und Netzwerken des ehemaligen Arbeitgebers. Auch wenn die Büroschlüssel fast immer kontrolliert eingezogen werden – die digitalen Schlüssel „passen“ oft noch über Tage und Wochen in die IT-Schlösser des Unternehmens – und manchmal bleiben so Zugänge für immer.

Experten gehen davon aus, dass fast ein Drittel ehemaliger Arbeitnehmer noch Zugang zu den Netzwerken ihres früheren Arbeitgebers haben. Das Risiko ist enorm.

Wenn ein Ex-Mitarbeiter noch Zugang hat zum Intranet, zu seinen E-Mail-Accounts, zum CRM-System, dann entscheidet nur Moral und Charakter über die IT-Sicherheit des Unternehmens. Mit bösem Willen wird der Diebstahl wert-voller Daten zum Kinderspiel. Informationen zu Produkten oder Kunden fließen ab, Sicherheitsprozesse werden manipuliert und Aufträge können verloren gehen. Eine Schnittstelle zum Personalsystem, worüber beim Austritt des Mitarbeiters auto-matisch und systemübergreifend von IAM die Accounts gesperrt werden, bietet Ihnen hier eine Lösung.



Der Human-Capital Management Connecter (HCM) sorgt für die Verbindung zwischen Personalsystem und der Benutzerverwaltung im Netzwerk (Quelle: Tools4ever).

Jan Pieter Giele: Seit 2004 als Geschäftsführer zuständig für Deutschland, Österreich und die Schweiz.

FRAGEN AN JAN PIETER GIELE

KOSTEN SPAREN – SICHERHEIT GEWINNEN DURCH IAM

HERR GIELE, WARUM IST BENUTZERMANAGEMENT AUCH SICHERHEITSMANAGEMENT?

Mit der DSGVO drohen bei Verstoß gegen Datenschutzrichtlinien empfindliche Bußgelder. Es ist das eine, dass Unbefugte grundsätzlich keinen Zugriff auf sensible Daten haben dürfen. Zudem muss das Unternehmen aber auch wissen, wer auf welche Daten Zugriff hat. Somit ist die Unterstützung durch IAM-Systeme notwendig, um die Sicherheitsanforderungen zu gewährleisten. Und Tools4ever liefert hier die Werkzeuge für Transparenz und Zugriffskontrolle in der Berechtigungsverwaltung.

WAS MACHT DIE TOOLS4EVER-LÖSUNG SO BESONDERS?

Wir passen unsere IAM-Lösung der Software-Umgebung unserer Kunden an und nicht umgekehrt. Und: Sie können mit unseren Lösungen direkt loslegen. Wir benötigen keine monatelange Konzeptphase. Unternehmen gehen mit Tools4ever auch kein Risiko ein – die IT-Experten können unsere IAM-Lösungen vor dem Erwerb in der eigenen IT-Umgebung ausgiebig testen.

WELCHE VORTEILE BRINGT IAM DEM UNTERNEHMER?

In unserer heutigen digitalen Welt mit immer mehr Systemen – On-Premise oder in der Cloud – entscheidet die richtige Verbindung von Menschen und Daten über den Unternehmenserfolg: Die Mitarbeiter müssen zu jeder Zeit und von überall Zugang zu den Daten haben, die sie für ihre Arbeit benötigen, und zwar einfach, schnell und sicher. Das gewährleistet Identity and Access Management – einfach eine sichere Methode, um dem Unternehmen durch effizienteres Arbeiten Zeit und Geld zu sparen.

TOOLS4EVER FEIERT DIESES JAHR 20-JÄHRIGES JUBILÄUM. WELCHES ENTWICKLUNGSPOTENTIAL SEHEN SIE IN SACHEN IAM FÜR DIE ZUKUNFT?

Tools4ever ist heute ein führender Entwickler und Anbieter von Identity Gover-nance & Administration-Lösungen und verwaltet mehr als 5 Millionen Konten für kleinere Unternehmen (ab 300 Benutzerkonten) und multinationale Unternehmen mit mehr als 200.000 Benutzern. Die Mitarbeiter arbeiten ständig daran, unsere Produkte für unsere Kunden zu verbessern.

Ein Beispiel: In Zukunft werden die meisten IT-Anwendungen von Unternehmen in der Cloud angelegt sein. Tools4ever hat mit HelloID schon heute eine benutzerfreundliche und sichere Identity and Access Management-Lösung dafür. Dank des Self-Service Tools wird die IT maßgeblich entlastet – neue Kapazitäten wer-den geschaffen und gleichzeitig Geld und Zeit gespart.

WER IST TOOLS4EVER?

Das niederländische Unternehmen mit Sitz in Baarn entwickelt und vertreibt Softwaresysteme für das Identity- und Access-Management (IAM). Weltweit vertrauen über 5.200 große und mittelständische Unternehmen aus allen Branchen auf die innovativen Lösungen von Tools4ever – von angepassten IAM-Komplettsystemen über integrierbare Softwaremodule bis zu speziellen Komponenten wie dem Berechtigungs- oder Passwortmanagement im Self-Service. Damit sorgt Tools4ever seit 20 Jahren für mehr Sicherheit, Transparenz und Effektivität im Benutzermanagement von Unternehmen mit mehr als 300 Computerarbeitsplätzen, vor Ort (On-Prem) und in der Cloud. Ihre IAM-Lösungen entlasten die IT-Abteilung, schaffen Kapazitäten und sparen Zeit und Geld. Die Tools4ever Informatik GmbH sitzt in Bergisch Gladbach und bietet IAM-Software, Dienstleistungen und Support im gesamten deutschsprachigen Raum.

TOOLS4EVER INFORMATIK GMBH

Hauptstraße 145 – 147
51465 Bergisch Gladbach
Deutschland

T +49 2202 2859 - 0 F +49 2202 2859 - 299

Information	info@tools4ever.de
Sales	sales@tools4ever.de
Support	projectdesk@tools4ever.de