Sicherheit und Datenschutz bei Workday

Einführung

Angesichts der zunehmenden Digitalisierung in Unternehmen gehört es zu den wichtigsten Aufgaben von IT-Führungskräften, Kunden-, Mitarbeiter- und urheberrechtlich geschützte Daten zu sichern und zu schützen. Zudem werden die Sicherheitsbedrohungen, mit denen Unternehmen heute konfrontiert sind, immer komplexer und machen Sicherheits- und Datenschutzkonzepte für sämtliche Aspekte des Service unerlässlich. Im Folgenden werden die Sicherheits- und Datenschutzpraktiken von Workday für IT-Experten erläutert.

Einhaltung gesetzlicher Bestimmungen und Zertifizierungen

Workday und unsere Kunden müssen eine Vielzahl internationaler Datenschutzvorschriften einhalten. Bestimmte Datenschutzgrundsätze, wie beispielsweise Informationspflicht, Wahlmöglichkeit, Zugriff, Nutzung, Offenlegung und Sicherheit, gelten in allen Rechtssystemen. Unsere Anwendung ist für unterschiedliche Konfigurationen ausgelegt, sodass Sie die in Ihrem Land geltenden Gesetze berücksichtigen können.

Darüber hinaus sorgt Workday mit einem umfassenden Informationssicherheitsprogramm (WISP) für die Einhaltung internationaler Datenschutzvorschriften. Dieses enthält technische und organisatorische Schutzmechanismen, die unbefugte Zugriffsversuche und Missbrauch oder Offenlegung von Kundendaten verhindern.

Externe Audits: SOC 1- und SOC 2-Prüfberichte

Die Aktivitäten, Richtlinien und Verfahren von Workday werden regelmäßig in Audits überprüft. So wird sichergestellt, dass Workday alle für Dienstleistungsanbieter relevanten Standards erfüllt und übertrifft. Workday veröffentlicht einen Service Organisation Control 1 (SOC 1) Typ II-Bericht. SOC 1 (vormals SAS 70) wird gemäß der Überwachungsnorm SSAE 18 (Statement on Standards for Attestation Engagements No. 18) und dem internationalen Prüfungsstandard für interne Kontrollsysteme ISAE 3402 (International Standard on Assurance Engagements No. 3402) ausgestellt.

Dieser Dual-Standard-Bericht bietet Unternehmen weltweit die Sicherheit, dass Dienstleistungsanbieter wie Workday angemessene Kontrollinstrumente einsetzen. Als Zielgruppe dieses Berichts informieren sich Kunden bzw. Interessenten über die internen Kontrollmechanismen für ausgelagerte kritische Geschäftsprozesse, die Auswirkungen auf ihre Finanzaufstellungen haben (Sarbanes-Oxley-Compliance). Der Geltungsbereich von SOC 1 ist auf die Produktionssysteme von Workday beschränkt und das SOC 1-Audit wird halbjährlich von einem unabhängigen externen Auditor durchgeführt. Der abschließende Bericht steht Kunden und Interessenten zur Verfügung.

Workday veröffentlicht darüber hinaus einen Service Organisation Control 2 (SOC 2) Typ II-Bericht. Der SOC 2-Bericht von Workday berücksichtigt sämtliche Grundsätze und Kriterien für vertrauenswürdige Dienstleistungen (Sicherheit, Verfügbarkeit, Vertraulichkeit, Verarbeitungsintegrität und Datenschutz). SOC 2 deckt alle Workday-Lösungen ab, die von Kunden an Workday Services übermittelte Daten enthalten. Dieser Bericht richtet sich an Kunden bzw. Interessenten, die sich über die internen Sicherheitskontrollen von Workday informieren möchten. Das SOC 2-Audit wird einmal jährlich von einem unabhängigen externen Auditor durchgeführt und Kunden und Interessenten anschließend als Bericht zur Verfügung gestellt.

Bei den Audits gemäß SOC 1 und SOC 2 werden die physischen und umgebungsbezogenen Schutzmechanismen validiert, die Workday in Produktionsrechenzentren, bei Backup- und Wiederherstellungsverfahren, in Softwareentwicklungsprozessen sowie bei logischen Sicherheitskontrollen einsetzt.

Zertifizierungen nach ISO 27001, 27017 und 27018

ISO 27001 ist eine Norm für Informationssicherheit, die 2005 von der Internationalen Organisation für Normung (ISO) und von der Internationalen Elektrotechnischen Kommission (IEC) veröffentlicht wurde. Im September 2013 wurde die ursprüngliche Norm aus dem Jahr 2005 durch ISO 27001:2013 ersetzt. ISO 27001 ist ein international anerkannter, normenbasierter Sicherheitsansatz, der die Anforderungen an ein unternehmenseigenes Managementsystem für Informationssicherheit (ISMS, Information Security Management System) definiert.

ISO 27017 wurde im Jahr 2015 veröffentlicht und ist eine ergänzende Norm zu ISO 27001. Diese Norm liefert Kontrollen und Implementierungsleitlinien für den Aspekt der Informationssicherheit bei der Bereitstellung und Nutzung von Cloud-Services.

ISO 27018 ist eine 2014 von ISO/IEC veröffentlichte ergänzende Norm. Sie beschreibt Leitlinien für Cloud-Services-Anbieter, die personenbezogene Daten verarbeiten.

Workday wurde im September 2010 nach ISO 27001, im Oktober 2015 nach ISO 27018 und im November 2017 nach ISO 27017 zertifiziert. Die Zertifizierung wird nach einer unabhängigen Beurteilung erteilt und bescheinigt Workday die Einhaltung der betreffenden ISO-Norm. Alle drei Jahre erfolgt die ISO-Rezertifizierung. Für die Aufrechterhaltung einer Zertifizierung sind zudem jährliche Überwachungsaudits erforderlich. Diese ISO-Zertifizierungen bekräftigen unsere Selbstverpflichtung zum Datenschutz und zur Sicherheit und belegen die Wirksamkeit der internen Kontrollen von Workday. Kunden haben Einsicht in die ISO-Zertifikate und die ISMS-Erklärung zur Anwendbarkeit (ISMS Statement of Applicability).

Grenzüberschreitende Datentransfers

Die Übermittlung personenbezogener Daten aus dem Europäischen Wirtschaftsraum (EWR) in die Vereinigten Staaten unterliegt strengen Datenschutzgesetzen. Um den Anforderungen der im EWR geschäftlich tätigen Kunden Rechnung zu tragen, hat Workday die von der Europäischen Kommission genehmigten Standardvertragsklauseln in seine Datenschutzvereinbarung übernommen. Die Standardvertragsklauseln schaffen einen Vertragsmechanismus, der die Anforderungen an ein angemessenes Datenschutzniveau für die Übermittlung personenbezogener Daten aus dem europäischen Wirtschaftsraum in ein Drittland erfüllt.

Zudem verfügt Workday über eine Selbstzertifizierung für die Rechtsinstrumente EU-US Privacy Shield (Datenschutzabkommen zwischen EU und USA) und Swiss-US Privacy Shield (Datenschutzabkommen zwischen Schweiz und USA). Der Privacy Shield ersetzt das Safe-Harbor-Abkommen und soll insbesondere die Schwachstellen beheben, aufgrund derer das Safe-Harbor-Abkommen vom Europäischen Gerichtshof für ungültig erklärt worden war. Workday nimmt aktiv am Privacy Shield-Verifizierungsprogramm teil. Die Verifizierung von Workday für den Privacy Shield erfolgt extern über TRUSTe.

Weitere Informationen zum Privacy-Shield-Programm des US-Handelsministeriums finden Sie unter http://www.privacyshield.gov. Details zu den vorgenannten Standardvertragsklauseln finden Sie unter http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm.

Weitere Informationen über das Engagement von Workday zum Schutz von Kundendaten sowie Einzelheiten zu unserem Datenschutzprogramm finden Sie in dem zugehörigen Datenblatt („Workday Privacy Program“).

Die Datenschutz-Grundverordnung

Die Datenschutz-Grundverordnung (DSGVO), eine Verordnung der Europäischen Union (EU), ersetzt die Datenschutzrichtlinie 95/46/EG sowie die Durchführungsbestimmungen der Mitgliedstaaten. Diese Verordnung trat am 25. Mai 2018 in allen 28 Mitgliedstaaten der EU in Kraft. Sie vereinfacht und vereinheitlicht die aktuellen Datenschutzgesetze in allen EU-Mitgliedstaaten. Die DSGVO gilt für Unternehmen in der EU ebenso wie für alle Unternehmen, die personenbezogene Daten von EU-Bürgern verarbeiten oder speichern. Der Sitz dieser Unternehmen ist dabei unerheblich.

Workday gilt im Sinne der DSGVO als Datenverarbeiter. Workday hat die Anforderungen der DSGVO umfassend bewertet und zahlreiche Datenschutz- und Sicherheitspraktiken eingeführt, um die Compliance mit der DSGVO als Datenverarbeiter von Grund auf sicherzustellen. Zu diesen Praktiken zählen u. a.:

- Weiterbildung von Mitarbeitern zu Sicherheits- und Datenschutzpraktiken
- Durchführung von Datenschutz-Folgeabschätzungen (Privacy Impact Assessments, PIA)
- Bereitstellung angemessener Datenübertragungsmethoden für unsere Kunden
- Aufzeichnung von Verarbeitungsaktivitäten
- Bereitstellung konfigurierbarer Datenschutz- und Compliance-Funktionen für unsere Kunden

Privacy by Design und Privacy by Default sind fest in Workday Services verankert. Uns ist bewusst, dass die DSGVO für die Geschäftstätigkeit unserer internationalen Kunden von zentraler Bedeutung ist. Workday verfolgt daher laufend die Leitlinien und Empfehlungen der EU-Aufsichtsbehörden im Zusammenhang mit der DSGVO und sorgt auf diese Weise dafür, dass sein Compliance-Programm stets auf dem neuesten Stand ist.

Datensicherheit

Physische Sicherheit

Workday betreibt seine Produktionssysteme in Co-Location-Rechenzentren, die dem neuesten Stand der Technik entsprechen und speziell für das Hosting unternehmenskritischer Rechnersysteme mit vollständig redundanten Teilsystemen sowie unterteilten Sicherheitszonen entwickelt wurden. Für die Rechenzentren von Workday gelten die strengsten physischen Sicherheitsmaßnahmen:

- Mehrere Authentifizierungsschichten für den Zutritt zum Serverbereich
- Biometrische Zwei-Faktor-Authentifizierung für sensible Bereiche
- Kameraüberwachungssysteme an kritischen internen und externen Eingängen
- 24/7-Überwachung der Rechenzentren durch Sicherheitspersonal
- Aufzeichnung und Überwachung unbefugter Zutrittsversuche durch den Sicherheitsdienst des Rechenzentrums

Sämtliche physischen Zutrittsmöglichkeiten zu den Rechenzentren sind stark eingeschränkt und werden streng überwacht. Bei den Datenoperationen von Workday kommen Best-Practice-Sicherheitsverfahren zur Anwendung, wie beispielsweise der Schutz von Servern durch besonders strenge Zugriffsrechte sowie regelmäßige Wartungsfenster.

Datentrennung

Workday ist eine mandantenfähige SaaS-Anwendung.

Die Mandantenfähigkeit ist ein Schlüsselmerkmal von Workday: Indem die Anwendungsdaten der einzelnen Kundenmandanten voneinander isoliert sind, können mehrere Kunden gemeinsam eine physische Instanz der Workday-Lösung nutzen. Workday setzt dies mithilfe des Workday Object Management Server (OMS) um. Jede Anwender-ID ist mit genau einem Mandanten verknüpft, über den der Zugriff auf die Workday-Anwendung erfolgt.

Alle Instanzen von Anwendungsobjekten (wie Organisation und Mitarbeiter) sind mandantenbasiert. Das heißt, jedes Mal, wenn ein neues Objekt erstellt wird, wird dieses Objekt ebenfalls untrennbar mit dem Mandanten des Anwenders verknüpft. Die Workday-Lösung behält diese Verknüpfungen automatisch bei und beschränkt den Zugriff auf jedes Objekt basierend auf der ID und dem Mandanten des Anwenders. Wenn ein Anwender Daten abruft, wendet die Lösung automatisch einen Mandantenfilter an, um sicherzustellen, dass sie nur diejenigen Informationen abruft, die dem Mandanten des Anwenders entsprechen.

Verschlüsselungsfunktion für gespeicherte Daten (Datenbanksicherheit)

Workday verschlüsselt jedes Kundendatenattribut innerhalb der Anwendung, bevor es in der Datenbank gespeichert wird. Dies ist ein wesentliches Designmerkmal der Workday-Technologie. Dabei setzt Workday den AES-Algorithmus (Advanced Encryption Standard) mit einer Schlüssellänge von 256 Bit ein. Diese Verschlüsselung ist in Workday realisierbar, weil es sich hierbei im Gegensatz zu festplattenbasierten RDBMS-Anwendungen um eine objektorientierte Anwendung mit In-Memory-Technologie handelt. Konkret bedeutet dies, dass die Metadaten in Workday vom Workday OMS interpretiert und im Speicher abgelegt werden. Alle Dateneinträge, -aktualisierungen und -löschungen werden in einen persistenten Speicher auf einer MySQL-Datenbank übertragen. Dank dieser einzigartigen Architektur arbeitet Workday mit nur einigen Dutzend Datenbanktabellen. Im Gegensatz dazu erfordert eine RDBMS-basierte Anwendung Zehntausende von Tabellen und macht eine Datenbankverschlüsselung aufgrund der nachteiligen Auswirkungen auf die Performance unmöglich.

Verschlüsselungsfunktion während der Datenübermittlung (Netzwerksicherheit)

Die Anwender greifen über das Internet auf die Workday-Anwendung zu. Dabei wird die Verbindung durch Transport Layer Security (TLS) geschützt. Auf diese Weise ist der Netzwerkverkehr gegen passive Lauschangriffe sowie aktive Manipulationen und Fälschungen von Nachrichten geschützt.

Workday hat außerdem proaktive Sicherheitsmechanismen wie Perimeterschutz- und Intrusion-Prevention-Systeme implementiert. Schwachstellenanalysen und Penetrationstests der Netzwerkinfrastruktur von Workday werden ebenfalls sowohl von internen Workday-Ressourcen als auch von externen Drittanbietern regelmäßig bewertet und durchgeführt.

Datensicherungen

Die primäre Produktionsdatenbank von Workday wird in Echtzeit auf eine Replikationsdatenbank repliziert, die sich in einem externen Rechenzentrum befindet. Von dieser Replikationsdatenbank wird jeden Tag ein vollständiges Backup durchgeführt. Gemäß unserer Datenbank-Backup-Richtlinie müssen Datenbanksicherungen und Transaktionsprotokolle in einem Umfang erfasst werden, der es erlaubt, eine Datenbank mit einem möglichst geringen Verlust an erfolgreich abgeschlossenen Transaktionen auf wirtschaftlich praktikable Weise wiederherzustellen. Die Transaktionsprotokolle werden so lange vorgehalten, bis auf den letzten Eintrag im Transaktionsprotokoll zwei Backups erfolgt sind. Datenbanksicherungen von Systemen, die Schnittstellen implementieren, müssen so lange verfügbar sein, wie es für die Unterstützung der über die Schnittstelle verbundenen Systeme erforderlich ist. Dieser Zeitraum variiert je nach System. Sicherungen der Datenbank- und Transaktionsprotokolle werden für alle Datenbanken verschlüsselt, die Kundendaten enthalten.

Disaster Recovery

Workday erbringt seinen Service gemäß seines Standard-Service-Level-Agreements (SLA). Das SLA enthält einen Disaster-Recovery-Plan (DR) für den Produktionsservice von Workday mit einer Zielvorgabe für die Wiederherstellungszeit (Recovery Time Objective, RTO) von 12 Stunden und einer Zielvorgabe für den Wiederherstellungspunkt (Recovery Point Objective, RPO) von einer Stunde. Die RTO definiert den Zeitraum ab dem Moment, wenn der Produktionsservice von Workday nicht mehr zur Verfügung steht, bis zu dem Zeitpunkt, an dem er wieder verfügbar ist. Die RPO definiert den Zeitraum ab dem Moment, wenn die erste Transaktion verloren geht, bis zu dem Zeitpunkt, an dem der Produktionsservice von Workday nicht mehr verfügbar ist.

Damit Workday die Verpflichtungen aus dem SLA einhalten kann, unterhält das Unternehmen eine DR-Umgebung mit einer vollständigen Replikation der Produktionsumgebung. Bei einem ungeplanten Ausfall, der voraussichtlich länger als eine vorher festgelegte Zeitspanne dauern wird, führt Workday den DR-Plan aus. Der DR-Plan wird mindestens alle sechs Monate getestet.

Ein einziges Sicherheitsmodell

Im Gegensatz zu ERP-Altsystemen arbeitet Workday mit einem einheitlichen Sicherheitsmodell. Dieses umfasst Anwenderzugriff, Systemintegration, Reporting, Mobilgeräte und IT-Zugriff. Jeder Nutzer muss sich über das Workday-Sicherheitsmodell anmelden und autorisiert werden. Bei ERP-Altsystemen gibt es dagegen meist eine Sicherheitsschicht für Anwendungen, die vom IT-Personal und den Datenbankadministratoren umgangen werden kann, um direkt auf Datenbankebene auf die Daten zuzugreifen. Dies ist bei Workday nicht möglich. Workday ist ein objektorientiertes In-Memory-System mit einem verschlüsselten persistenten Datenspeicher. Damit ist gewährleistet, dass Zugriffsereignisse und -änderungen nachverfolgt und geprüft werden. Da außerdem alle Datenupdates automatisch mit einem Gültigkeitsdatum versehen und geprüft werden, kann mit diesem einzigartig robusten Sicherheitsmodell der Zeit- und Kostenaufwand von Governance und Compliance erheblich verringert und das allgemeine Sicherheitsrisiko reduziert werden.

Authentifizierung

Der Sicherheitszugriff bei Workday ist rollenbasiert. Er unterstützt SAML für einmaliges Anmelden (Single Sign-On, SSO) und X.509-Zertifikatauthentifizierung sowohl für Anwender- als auch für Webservices-Integrationen. Mit Workday können Kunden für verschiedene Anwendergruppen unterschiedliche Authentifizierungsanforderungen festlegen.

Außerdem können Anwender in Workday einen Authentifizierungstyp auswählen, wenn Unternehmen aufgrund unterschiedlicher geografischer Standorte oder Organisationen verschiedene Authentifizierungsarten für Anwender wünschen.

Single Sign-On

Während LDAP eine einheitliche Anmeldung mit Benutzername und Kennwort ermöglicht, geht SAML einen Schritt weiter und unterstützt eine SSO-Umgebung für Unternehmen. SAML ermöglicht eine nahtlose SSO-Interaktion zwischen der internen IAM-Lösung (Identity and Access Management) des Kunden und Workday.

Systemeigene Workday-Anmeldung

Für Kunden, die die systemeigene Anmeldung nutzen möchten, wird das Workday-Kennwort nur in Form eines sicheren Hashwerts anstelle des Kennworts selbst in Workday gespeichert. Erfolglose Anmeldeversuche sowie erfolgreiche Anmelde-/Abmeldeaktivitäten werden zu Audit-Zwecken protokolliert. Inaktive Anwendersitzungen werden nach einer bestimmten Zeit automatisch beendet. Die Zeit kann vom Kunden nach Anwender konfiguriert werden. Zu den Kennwortregeln, die der Kunde konfigurieren kann, gehören Länge, Komplexität und Laufzeit.

Multi-Faktor-Authentifizierung

Workday bietet eine Multi-Faktor-Authentifizierung (MFA) und empfiehlt Kunden, diese zu nutzen. Dazu können sie in Workday jede beliebige Authenticator-App zur Verfügung zu stellen, die durch den TOTP-Algorithmus (Time-Based One-Time Passcode) unterstützt wird. Mit diesem Setup können die Kunden MFA-Anbieter ganz einfach in die systemeigene Workday-Anmeldung integrieren. Darüber hinaus bietet Workday den Endanwendern seiner Kunden die Möglichkeit, über einen E-Mail-zu-SMS-Gateway-Mechanismus einen einmaligen Passcode zu erhalten. Zu guter Letzt unterstützt Workday auch Sicherheitsfragen als zusätzlichen Mechanismus zur Feststellung der Anwenderidentität.

Vertrauenswürdige Geräte

Workday bietet seinen Kunden und deren Endanwendern die Möglichkeit, Geräte als vertrauenswürdig für den Zugriff auf ihren Workday-Mandanten zu definieren. Die Endanwender werden benachrichtigt, sobald jemand versucht, sich über nicht zugelassene Geräte Zugang zu ihrem Konto zu verschaffen. Geräte, die nicht mehr als vertrauenswürdig betrachtet werden, können von den Endanwendern entfernt werden. Administratoren wird eine Liste der vertrauenswürdigen Geräte für Überwachungszwecke zur Verfügung gestellt. Damit Administratoren diese Funktion konfigurieren können, müssen sie sie für ihren Mandanten aktivieren. Endanwender müssen der Nachverfolgung des vertrauenswürdigen Geräts per Browser-Cookie zustimmen.

Step-up-Authentifizierung

Als stärkeren Authentifizierungsmechanismus für den Zugang zu sensiblen Ressourcen stellt Workday die Step-up-Authentifizierung bereit. Unternehmen, die eine SAML-Authentifizierung nutzen, können zusätzlich dafür sorgen, dass ihre Daten vor unbefugtem Zugriff auf Elemente geschützt werden, die in Workday als kritisch eingestuft sind. So können Kunden einen zweiten Authentifizierungsfaktor festlegen, den Anwender für den Zugriff auf diese Elemente eingeben müssen.

Autorisierung

Die Workday-Anwendung setzt bei der Autorisierung Sicherheitsrichtlinien auf der Basis von Gruppen durch. Die Anwendung verhindert, dass Anwender direkt auf die Produktionsdatenbank zugreifen können. In Kombination mit vordefinierten Sicherheitsrichtlinien gewähren oder beschränken von Workday bereitgestellte und vom Kunden erstellte Sicherheitsgruppen den Anwenderzugriff auf Funktionen, Geschäftsprozesse, Berichte und Daten – unabhängig davon, ob der Zugriff online oder über Webservices erfolgt.

Die vom Kunden konfigurierbaren Sicherheitsgruppen können auf Basis von Anwendern, Rollen, Tätigkeiten, Organisationen, Standorthierarchie oder Niederlassungen definiert werden. Sie können zu neuen Sicherheitsgruppen kombiniert werden, die andere Gruppen logisch ein- und ausschließen. Der System-to-System-Zugriff wird über Sicherheitsgruppen für das Integrationssystem definiert. Kunden können diese Gruppen und Richtlinien an ihre konkreten Anforderungen anpassen und den Zugriff so fein justieren, wie es für die Unterstützung komplexer Konfigurationen, einschließlich globaler Deployments, erforderlich ist.

Workday stellt zudem Sicherheitsgruppen bereit, die automatisch auf der Basis von Geschäftsprozessen wie Einstellung und Vertragsbeendigung aktualisiert werden. Diese von Workday bereitgestellten Gruppen können einzeln oder in Kombination mit anderen von Workday bereitgestellten oder vom Kunden erstellten Sicherheitsgruppen genutzt werden, um den Zugriff anhand von Sicherheitsrichtlinien festzulegen.

Public Cloud

Workday nutzt Public-Cloud-Services von Amazon Web Services (AWS) zum Speichern und Verarbeiten von Inhalten in Workday Media Cloud. Die Inhalte der Kunden werden logisch voneinander getrennt. Sämtliche Inhalte von Workday Media Cloud werden im gespeicherten Zustand durch die serverseitige Verschlüsselung von AWS gesichert. Jedes Objekt, das Workday in AWS speichert, wird mit einem eindeutigen 256-Bit-AES-Verschlüsselungscode gesichert.

Workday nutzt Amazon Virtual Private Cloud (Amazon VPC), einen logisch getrennten Abschnitt der AWS-Cloud. Die gesamte Kommunikation zwischen Endanwendern und Workday-Rechenzentren sowie Workday Amazon VPC-Services wird auf der Transportschicht verschlüsselt. Ebenso wird die gesamte Kommunikation von Workday Amazon VPC-Services an Workday-Rechenzentren und umgekehrt verschlüsselt. Workday verwendet das TLS-Protokoll, um den gesamten Datenverkehr ausschließlich mit sicheren Chiffren zu verschlüsseln.

Lückenlose Audits

Workday protokolliert sämtliche Änderungen an Geschäftsdaten auf der Anwendungsebene. Diese Informationen zur Anwendungsüberwachung bilden die Grundlage für Audit- und Compliance-Reporting innerhalb der gesamten Workday-Lösung. Workday erfasst erfolgreiche An- und Abmeldungen von Anwendern sowie fehlgeschlagene Anmeldeversuche und stellt diese Informationen in Workday-Auditberichten bereit. Workday verwendet nicht-destruktive Updates – das bedeutet, dass die Daten nie überschrieben werden, sondern für die gesamte Lebensdauer des Mandanten erhalten bleiben. Den Kunden steht damit bei Bedarf eine vollständige, detaillierte Audithistorie zur Verfügung. Über die Auditfunktionen in Workday erhalten Auditoren alle erforderlichen Informationen, um die Änderungshistorie eines Geschäftsobjekts oder einer Transaktion nachzuverfolgen.

Über Workday

Workday ist ein führender Anbieter von Enterprise-Cloud-Anwendungen für das Finanz- und Personalwesen.

Das 2005 gegründete Unternehmen bietet weltweit Anwendungen in den Bereichen Finanzmanagement, Human Capital Management und Analyse, die für globale Konzerne, Bildungseinrichtungen und Regierungsbehörden konzipiert sind. Von mittelständischen bis hin zu *Fortune*-50-Unternehmen haben sich Organisationen bereits für Workday entschieden.

Workday | Telefon: 49 (0) 89 21093215 | workday.de