Beveiliging en dataprivacy bij Workday

Inleiding

Bedrijven worden steeds digitaler. Daarom staat het beveiligen en beschermen van klant-, werknemers- en intellectuele-eigendomsdata hoog op de agenda van IT-managers. Omdat organisaties te maken krijgen met meer complexe beveiligingsrisico's, is het van cruciaal belang om beveiliging en dataprivacy te bieden op alle vlakken van onze services. In deze introductie voor IT-professionals leest u hoe Workday beveiliging en dataprivacy in praktijk brengt.

Naleving van wet- en regelgeving en certificeringen

Workday en onze klanten moeten zich houden aan verschillende internationale privacyregels. De algemene privacybeginselen in de verschillende jurisdicties zijn kennisgeving, keuze, toegang, gebruik, openbaarmaking en beveiliging. Onze applicatie is ontworpen om gedifferentieerde configuraties te kunnen implementeren, zodat u de specifieke wetgeving van uw land kunt naleven.

Workday leeft internationale privacywetgeving na door continu te werken aan een uitgebreid, schriftelijk informatiebeveiligingsprogramma met technische en administratieve maatregelen om onbevoegde toegang, ofonbevoegd gebruik of openbaarmaking van klantdata te voorkomen.

Externe audits: SOC 1- en SOC 2-rapporten

De activiteiten, het beleid en de procedures van Workday worden regelmatig gecontroleerd. Zo wordt gegarandeerd dat Workday voldoet aan alle standaarden die worden verwacht van serviceproviders, en deze zelfs overtreft. Workday publiceert een rapport over Service Organization Controls 1 (SOC 1) Type II. SOC 1 is de opvolger van SAS 70 en wordt afgegeven in overeenstemming met SSAE 18 (Statement on Standards for Attestation Engagements No. 18) en ISAE 3402 (International Standard on Assurance Engagements No. 3402)

Dit rapport verschaft bedrijven overal ter wereld de zekerheid dat een serviceprovider, zoals Workday, de juiste maatregelen heeft geïmplementeerd. Dit rapport is bestemd voor klanten of prospects die inzicht moeten hebben in interne controles op uitbestede cruciale bedrijfstaken die een impact kunnen hebben op de financiële verslagen van een klant (naleving van Sarbanes-Oxley). SOC 1 beperkt zich tot de productiesystemen van Workday. Een onafhankelijke externe auditor voert elke zes maanden een SOC 1-audit uit. Het rapport is na afronding beschikbaar voor klanten en prospects.

Workday publiceert ook een SOC 2 (Service Organization Controls 2) Type II-rapport. In het SOC 2-rapport van Workday worden alle principes en criteria voor trust services (beveiliging, beschikbaarheid, vertrouwelijkheid, verwerkingsintegriteit en privacy) behandeld. SOC 2 gaat over alle Workday-systemen die data bevatten die klanten hebben verzonden naar Workday Services. Dit rapport is bestemd voor klanten of prospects die graag meer inzicht willen in de interne beveiligingsmaatregelen van Workday. De SOC 2-audit wordt eenmaal per jaar uitgevoerd door een onafhankelijke externe auditor en klanten of prospects kunnen de resultaten inzien.

De SOC 1- en SOC 2-audits valideren Workday's fysieke en milieumaatregelen voor productiedatacenters, back-up- en herstelprocedures, softwareontwikkelingsprocessen en logische beveiligingscontroles.

ISO 27001-, 27017- en 27018-certificeringen

ISO 27001 is een standaard voor informatiebeveiliging die oorspronkelijk in 2005 is gepubliceerd door de International Organization for Standardization (ISO) en de International Electrotechnical Commission (IEC). ISO 27001:2013 werd gepubliceerd in september 2013 en vervangt de oorspronkelijke standaard uit 2005. ISO 27001 is een wereldwijd erkende, op standaarden gebaseerde benadering van beveiliging waarin de vereisten worden vermeld voor de Information Security Management Systems (ISMS), oftewel systemen voor informatiebeveiligingsmanagement van organisaties.

ISO 27017 werd gepubliceerd in 2015 en is een aanvulling op ISO 27001. Deze standaard biedt maatregelen en implementatierichtlijnen voor informatiebeveiliging die van toepassing zijn op het leveren en gebruiken van cloudservices.

ISO 27018 is een aanvullende standaard die in 2014 door ISO/IEC is gepubliceerd. ISO 27018 bevat richtlijnen die van toepassing zijn op providers van cloudservices die persoonsgegevens verwerken.

Workday ontving in september 2010 de certificering voor ISO 27001, in oktober 2015 die voor ISO 27018 en in november 2017 de certificering voor ISO 27017. De certificering wordt verkregen na een onafhankelijke beoordeling van de naleving van de ISO-standaard door Workday. ISO-hercertificering vindt elke drie jaar plaats, maar om een certificering te behouden, moet het bedrijf jaarlijkse controle-audits ondergaan. Deze ISO-certificeringen laten zien hoe belangrijk privacy en beveiliging voor ons zijn, en tonen aan dat onze maatregelen effect hebben. De ISO-certificaten en de ISMS Statement of Applicability kunnen door klanten worden ingezien.

Grensoverschrijdende overdracht van data

Op de overdracht van persoonlijke gegevens vanuit de Europese Economische Ruimte (EER) naar de Verenigde Staten zijn strenge gegevensbeschermingswetten van toepassing. Om te zorgen dat onze klanten met activiteiten in de EER aan deze vereisten voldoen, heeft Workday de goedgekeurde standaardcontractclausules van de Europese Commissie, ook wel het modelcontract genoemd, opgenomen in onze Data Protection Agreement. Het modelcontract zorgt voor een mechanisme om te voldoen aan de vereisten op grond waarvan de overdracht van persoonlijke gegevens vanuit de EER naar een derde land wordt toegestaan.

Workday heeft zich ook geconformeerd aan het Privacy Shield van de EU en de VS en van het Privacy Shield van Zwitserland en de VS. Het Privacy Shield vervangt het Safe Harbor Framework en is specifiek bedoeld voor de probleemkwesties die het Europese Hof van Justitie heeft vastgesteld tijdens de uitspraak waarin het Safe Harbor Framework ongeldig werd verklaard. Workday is een actieve deelnemer aan het Privacy Shield-programma. Workday gebruikt TRUSTe als onafhankelijke verificatiemethode voor het Privacy Shield.

Meer informatie over het Privacy Shield-programma van het U.S. Department of Commerce is te vinden op http://www.privacyshield.gov. Meer informatie over de standaardcontractclausules is te vinden op http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm.

Meer informatie over ons privacyprogramma en hoe Workday de dataprivacy van onze klanten beschermt, is te vinden in het datasheet over het privacyprogramma van Workday.

De General Data Protection Regulation (GDPR/AVG)

De GDPR is een verordening van de Europese Unie die de Richtlijn 95/46/EC inzake gegevensbescherming intrekt en vervangt, evenals de uitvoeringswetgeving van de lidstaten. Deze verordening werd in alle 28 EU-lidstaten van kracht op 25 mei 2018 en stroomlijnt de huidige regelgeving met betrekking tot gegevensbescherming in alle EU-lidstaten. De GDPR is zowel van toepassing op bedrijven in de EU als op alle bedrijven die de persoonlijke gegevens van EU-burgers verwerken of opslaan, ongeacht waar ze zich bevinden.

Volgens de GDPR is Workday een verwerker van data (data processor). Workday heeft de GDPR uitgebreid geëvalueerd en heeft een groot aantal privacy- en beveiligingsmaatregelen getroffen om vanaf het eerste moment te kunnen voldoen aan de eisen voor verwerkers van data (data processor compliance). Deze maatregelen zijn o.a.:

- Werknemers trainen op het gebied van beveiliging en privacy
- Privacy impact assessments uitvoeren
- Onze klanten voorzien van voldoende datatransfer-methoden
- Het verwerken van gegevens vastleggen
- Onze klanten configureerbare privacy- en compliancefuncties bieden

Privacy by Design en Privacy by Default zijn concepten die diep verankerd zijn in Workday Services. Omdat we weten dat de GDPR een belangrijke prioriteit is voor onze internationale klanten, blijft Workday de richtlijnen die de toezichthoudende instanties van de EU uitgeven met betrekking tot de GDPR monitoren, om er zeker van te zijn dat ons compliance-programma up-to-date is.

Databeveiliging

Fysieke beveiliging

Workday heeft haar productiesystemen ondergebracht in state-of-the-art datacenters die zijn ontworpen voor het hosten van bedrijfskritische computersystemen met volledig meervoudige subsystemen en gescheiden beveiligingszones. De datacenters van Workday zijn voorzien van de strengste fysieke beveiligingsmaatregelen:

- Meerdere authenticatielagen voordat toegang tot de serverruimte wordt verleend.
- Voor cruciale ruimtes is dubbele biometrische authenticatie vereist.
- Op cruciale interne en externe toegangspunten zijn camerabewakingssystemen geplaatst.
- De datacenters staan 24/7 onder toezicht van beveiligingspersoneel.
- Pogingen tot onbevoegde toegang worden geregistreerd en bewaakt door data center security.

Alle fysieke toegang tot de datacenters is zeer beperkt en streng gereguleerd. Voor de data-activiteiten van Workday wordt gebruikgemaakt van best practices op beveiligingsgebied, zoals beveiligde servers waarvoor alleen strikt noodzakelijke toegangsrechten worden verleend en regulier onderhoud dat is ingepland in onderhoudsvensters.

Data segregration

Workday is een multitentant SaaS-applicatie.

Multitenancy is een belangrijke functie van Workday waarmee meerdere klanten één fysieke instantie van het Workday-systeem kunnen delen terwijl de applicatiedata van elke klant gescheiden blijft. Workday maakt dit mogelijk via de Workday Object Management Server (OMS). Elke gebruikers-id wordt gekoppeld aan exact één tenant, die vervolgens wordt gebruikt voor toegang tot de Workday-applicatie.

Alle instanties van applicatie-objecten (zoals organisatie en medewerker) zijn tenantgebaseerd, zodat telkens als een nieuw object wordt gemaakt, dat object ook onherroepelijk wordt gekoppeld aan de tenant van de gebruiker. Deze koppelingen worden automatisch beheerd door het Workday-systeem, waarmee toegang tot elk object wordt beperkt op basis van de gebruikers-id en tenant. Wanneer een gebruiker data opvraagt, wordt automatisch een filter toegepast om te garanderen dat alleen data wordt opgehaald overeenkomstig met de tenant van de gebruiker.

Versleuteling van gegevens in opslag (databasebeveiliging)

Workday encrypt elk attribuut van customer data binnen de applicatie voordat data in de database wordt opgeslagen. Dit is een fundamenteel kenmerk van het ontwerp van de Workday-technologie. Workday maakt gebruik van het AES-algoritme (Advanced Encryption Standard) met een sleutelgrootte van 256 bits. Workday kan deze encryptie bereiken omdat het een in-memory objectgeoriënteerde applicatie is, in tegenstelling tot een disk-based RDBMS-aplicatie. Om precies te zijn: de metadata van Workday wordt geïnterpreteerd door de Workday OMS en in het geheugen opgeslagen. Alle data insert, -updates en -deletes worden vastgelegd in een persistent store in een MySQL-database. Deze unieke architectuur houdt in dat Workday slechts met enkele tientallen database tabellen werkt. Een op RDBMS gebaseerde applicatie heeft daarentegen tienduizenden tabellen nodig, waardoor volledige databaseversleuteling onpraktisch wordt vanwege de nadelige invloed hiervan op de prestaties.

Encryptie van data tijdens verzending (netwerkbeveiliging)

Gebruikers hebben toegang tot Workday via een internetverbinding die beveiligd is met TLS (Transport Layer Security). Dit garandeert dat het netwerkverkeer is beveiligd tegen passief afluisteren, actieve sabotage en vervalsing van berichten.

Workday heeft ook proactieve beveiligingsprocedures geïmplementeerd, zoals perimeterbeveiliging en systemen om het netwerk te beschermen tegen indringers. Daarnaast worden regelmatig kwetsbaarheidsanalyses en penetratietests van de Workday-netwerkinfrastructuur geëvalueerd en uitgevoerd, zowel door interne resources van Workday als door externe bedrijven.

Back-up van data

De primaire productiedatabase van Workday wordt in realtime gerepliceerd naar een replicadatabase in een datacenter op een andere locatie. Van deze replicadatabase wordt dagelijks een volledige back-up gemaakt. Op grond van ons back-upbeleid moeten databaseback-ups en transactielogs worden gemaakt, zodat een database kan worden hersteld met verlies van zo weinig geregistreerde transacties als commercieel haalbaar is. Transactielogs worden bewaard totdat er twee back-ups van de data zijn na de laatste invoer in het transactielog. Databaseback-ups van systemen die interfaces implementeren, moeten zo lang beschikbaar zijn als nodig is om de interfacing-systemen te ondersteunen. Deze periode varieert per systeem. Back-ups van de database en transactielogs worden versleuteld voor elke database die klantgegevens bevat.

Disaster Recovery

Workday garandeert haar service volgens haar standaard SLA (Service Level Agreement). De SLA bevat een disaster recovery (DR) plan voor de Workday Production Service met een RTO (Recovery Time Objective) van twaalf uur en een RPO (Recovery Point Objective) van één uur. De RTO wordt gemeten vanaf het moment dat de Workday Production Service niet meer beschikbaar is totdat deze weer beschikbaar is. De RPO wordt gemeten vanaf het moment waarop de eerste transactie verloren is gegaan tot het moment waarop de Workday Production Service niet meer beschikbaar was.

Om te garanderen dat Workday zich aan deze SLA-verplichtingen houdt, onderhoudt Workday een noodherstelomgeving met een volledige replica van de productieomgeving. In het geval van ongeplande uitval waarbij de uitval naar schatting langer duurt dan een vooraf gedefinieerde duur, voert Workday het noodherstelplan uit. Het noodherstelplan wordt minimaal elke zes maanden getest.

Eén beveiligingsmodel

In tegenstelling tot oudere ERP-systemen werkt Workday met één beveiligingsmodel. Hieronder vallen gebruikerstoegang, systeemintegratie, rapportage, mobiele devices en IT-toegang. Iedereen moet zich aanmelden en wordt geautoriseerd via het Workday-beveiligingsmodel. De beveiliging in legacy ERP-systemen kent meestal een applicatielaag voor beveiliging die door IT- en DBA-personeel kan worden omzeild om de data rechtstreeks op databaseniveau te openen. Met Workday is dat niet mogelijk. Workday is een objectgeoriënteerd, in-memory systeem met een versleutelde permanente gegevensopslag. Hierdoor kunnen alle toegang en wijzigingen worden getraceerd en gecontroleerd. Dankzij dit unieke robuuste beveiligingsmodel, gecombineerd met de automatische functie om alle gegevensupdates van een ingangsdatum te voorzien en te controleren, kosten governance en compliance minder tijd en geld en worden de beveiligingsrisico's gereduceerd.

Authenticatie

De beveiligingstoegang van Workday is gebaseerd op rollen en biedt ondersteuning voor SAML voor single-sign on (SSO) en x509-certificaatauthenticatie voor user en web services integraties. Met Workday kunnen klanten verschillende authenticatie-vereisten instellen voor verschillende gebruikerspopulaties.

Ook biedt Workday gebruikers de mogelijkheid om een authenticatietype te selecteren in situaties waarin organisaties meerdere authenticatietypen willen gebruiken vanwege geografische en/of organisatieverschillen.

Single-Sign-On Support

Terwijl LDAP de mogelijkheid biedt tot een geünificeerde gebruikersnaam/wachtwoordoplossing, gaat SAML een stap verder door het mogelijk maken van een SSO-omgeving (single sign-on). SAML zorgt voor een naadloze SSO-ervaring tussen de interne oplossing van de klant voor identiteits- en access management (IAM) en Workday.

Workday Native Login

Voor klanten die native login willen gebruiken slaat Workday alleen hun Workday-wachtwoord op in de vorm van een beveiligde hash, en dus niet het wachtwoord zelf. Voor auditdoeleinden worden zowel niet-geslaagde loginpogingen als geslaagde login/loguitactiviteiten geregistreerd. Voor inactieve gebruikerssessies treedt na een bepaalde tijd automatisch een time-out op, die door de klant kan worden geconfigureerd per gebruiker. Wachtwoordregels die door de klant kunnen worden geconfigureerd, zijn onder meer de lengte, de complexiteit en de vervaldatum.

Multifactor Authentication

Workday adviseert haar klanten gebruik te maken van meervoudige authenticatie (MFA). Workday biedt klanten de mogelijkheid om eender welke authenticatie-applicatie die wordt ondersteund door het Time-Based One Time Passcode (TOTP)-algoritme te gebruiken. Met deze instelling kunnen klanten eenvoudig een MFA-provider integreren in Workday Native Login. Workday biedt eindgebruikers van klanten ook de mogelijkheid om een eenmalige wachtwoordcode te ontvangen via een e-mail-naar-sms-gateway. Ten slotte ondersteunt Workday ook beveiligingsvragen als extra laag om de identiteit van een gebruiker te bevestigen.

Trusted Devices

Met Workday kunnen klanten en hun eindgebruikers devices aanmelden als 'vertrouwd' en op deze manier toegang krijgen tot hun Workday-tenant. Eindgebruikers ontvangen een bericht als een niet-herkend device toegang probeert te krijgen tot hun account. Ook kunnen ze devices verwijderen die ze niet langer vertrouwen. Administrators ontvangen een lijst met vertrouwde devices zodat ze deze kunnen bewaken. Als een administrator deze functie wil configureren, moet hij of zij deze inschakelen voor hun tenant. Eindgebruikers moeten dan toestemming geven voor het volgen van het vertrouwde device met een browsercookie.

Step-Up Authentication

Workday biedt step-up authentication als een krachtigere manier van authenticatie voor de meest gevoelige resources. Organisaties die SAML gebruiken als authenticatiemiddel, kunnen nog beter garanderen dat data beveiligd is tegen onbevoegde toegang tot kritische items in Workday. Hiermee kunnen klanten een tweede authenticatie afdwingen die gebruikers moeten invoeren om toegang tot die items te krijgen.

Autorisatie

De Workday-applicatie hanteert group-policy based security voor autorisatie. De applicatie voorkomt dat gebruikers direct toegang hebben tot de productiedatabase. Op grond van de beveiligingsgroepen die worden geleverd door Workday en gemaakt door de klant, in combinatie met vooraf gedefinieerd beveiligingsbeleid, wordt aan gebruikers toegang verleend of beperkt tot functie, bedrijfsprocessen, rapporten en data, hetzij online of via webservices.

Beveiligingsgroepen die door de klant worden geconfigureerd zijn gebaseerd op gebruikers, rollen, functies, organisaties, hiërarchie van de locatie of bedrijfslocaties. Ze kunnen worden gecombineerd in nieuwe beveiligingsgroepen die op basis van logica groepen opnemen of uitsluiten. Systeem-tot-systeem-toegang wordt gedefinieerd door beveiligingsgroepen op basis van integratiesystemen. Klanten kunnen deze groepen en dit beleid aanpassen aan hun behoeften en een zo fijnmazige toegang bieden als vereist is voor de ondersteuning van complexe configuraties, inclusief internationale implementaties.

Workday biedt ook beveiligingsgroepen die automatisch worden bijgewerkt op basis van bedrijfsprocessen, zoals het aannemen van nieuw personeel of het beëindigen van een arbeidsovereenkomst. Deze door Workday geleverde groepen kunnen op zichzelf worden gebruikt of in combinatie met andere beveiligingsgroepen van Workday of van de klant om toegang te verlenen volgens het beveiligingsbeleid.

Public cloud

Workday gebruikt public cloudservices van Amazon Web Services (AWS) om content op te slaan en te verwerken in Workday Media Cloud. De content van klanten is op een logische manier gescheiden van die van andere klanten. Alle Workday Media Cloud-content is passief versleuteld door middel van de encryptie in de server van AWS. Elk object dat Workday opslaat in AWS is versleuteld met AES door middel van een unieke encryptiesleutel van 256 bits.

Workday maakt gebruik van Amazon Virtual Private Cloud (Amazon VPC), wat een logisch geïsoleerde sectie van de AWS-cloud is. Alle communicatie tussen eindgebruikers, Workday-datacenters en Workday Amazon VPC-services is versleuteld in de transportlaag. Bovendien is ook alle communicatie van Workday Amazon VPC-services naar Workday-datacenters en vice versa versleuteld. Workday maakt gebruik van het TLS-protocol om al het verkeer met veilige sleutels te versleutelen.

Always-on auditing

Workday houdt alle wijzigingen van bedrijfsdata bij op applicatieniveau. Deze applicatie-auditinformatie is de basis voor audit- en compliance-rapporten in het hele Workday-systeem. Workday houdt geslaagde logins en logouts door gebruikers bij, evenals niet-geslaagde logins, en maakt dit inzichtelijk via Workday-auditrapporten. Workday maakt gebruik van nondestructive updates. Dat betekent dat data nooit wordt overschreven, en wordt behouden gedurende de hele levensduur van de tenant. Hierdoor beschikken klanten over een volledige auditgeschiedenis van elke waarde. Dankzij de auditfuncties in Workday beschikt een auditor over de informatie die nodig is om de wijzigingen die zijn aangebracht aan een business object of transactie te kunnen terugzien.

Over Workday

Workday is een toonaangevend leverancier van enterprise cloud applicaties voor finance en HR.

Workday is in 2005 opgericht en biedt applicaties voor finance management, human capital management en analytics, ontwikkeld voor 's werelds grootste bedrijven, opleidingsinstituten en overheidsinstellingen. Zowel middelgrote bedrijven als *Fortune* 50-ondernemingen hebben voor Workday gekozen.

Workday | Telefoonnummer: +31 (0)20 808 1836 | workday.com/nl