UKG Pro Workforce Management in de Google Cloud

Veiligheid, privacy en technologie

Inleiding

Nu steeds meer organisaties de IT voor hun kernactiviteiten naar de cloud verplaatsen, moeten ze erop kunnen vertrouwen dat cloudproviders de industriestandaarden voor beveiliging van hun gehoste applicaties strikt naleven of zelfs overtreffen. UKG™ (Ultimate Kronos Group) zorgt dat uw gehoste oplossing steeds online en beschikbaar is door gebruik te maken van de modernste technologieën voor beveiliging en onderhoud van de applicaties.

UKG ontwerpt en implementeert systemen en processen voor workforce management die de privacy van persoonlijke informatie beschermen in alle fasen van de dataverwerking.

Certificeringen en standaarden

UKG Pro Workforce Management™ wordt geïmplementeerd in het Google™ Cloud Platform (GCP), dat beschikt over certificeringen volgens ISO 27001, ISO 27017 en ISO 27018. GCP wordt jaarlijks door een onafhankelijke auditfirma gecontroleerd volgens de criteria van AICPA SSAE 18 SOC 2 en beschikt over een FedRAMP-certificering. De applicaties en services van UKG Pro Workforce Management zijn gecertificeerd volgens ISO 27001, ISO 27017 en ISO 27018. UKG Pro Workforce Management wordt eveneens jaarlijks getoetst aan de AICPA SSAE 18 Trust Principles voor veiligheid, vertrouwelijkheid, beschikbaarheid, verwerkingsintegriteit en privacy. De SOC 2 Type II-rapporten over UKG Pro Workforce Management en de SOC 2-rapporten over Google Cloud Platform zijn op aanvraag beschikbaar na ondertekening van een wederzijdse geheimhoudingsovereenkomst.

Privacy

Als technologieleider op het gebied van personeelsoplossingen begrijpt UKG de regeldruk waarmee onze klanten te maken hebben op het veranderlijke gebied van persoonlijke privacy. In het kader van onze filosofie om de klant altijd voorop te plaatsen, ontwerpt en implementeert UKG systemen en processen voor personeelsbeheer die de privacy van persoonlijke informatie in alle fasen van de gegevensverwerking beschermen volgens de instructies van onze klanten, ons eigen privacybeleid en alle toepasselijke wet- en regelgeving.

Privacycultuur

Privacy begint bij UKG aan de top. De commitment en steun van de directie hebben geleid tot een betere bewustwording bij onze medewerkers en tot processen die de gegevensbescherming en de privacy van persoonlijke informatie bevorderen.

Rapportage over verwerking

Het proces voor data-inventarisatie van UKG is ontworpen met het oog op zeer nauwkeurige rapportage van de verwerkingsactiviteiten wij namens onze klanten uitvoeren.

Gegevensverwerking

UKG neemt technische en organisatorische maatregelen om te zorgen dat onze klanten al hun verplichtingen voor gegevensbescherming uit hoofde van de Europese Algemene verordening gegevensbescherming (AVG) kunnen nakomen.

Privacy-effectbeoordelingen

Terwijl we onze producten en processen verder ontwikkelen, blijft UKG de privacy beoordelen en risicogebieden identificeren volgens ons systeem voor inventarisatie en classificatie van data.

Beheer van leveranciersrisico

UKG beheerst het leveranciersrisico door middel van toezicht en contractuele afspraken om te zorgen dat ook onze externe partners de gegevens verwerken volgens de AVG-principes van de Europese Unie.

Incidentenbeheer

Op basis van het UKG Cybersecurity Incident Response Plan reageren wij met grote urgentie op mogelijke incidenten rond persoonlijke informatie.

Encryptie: protocollen en cryptografie

Data in transit: Data voor web- en mobiele applicaties, API's en terminalcommunicatie worden beschermd met TLS (Transport Layer Security). UKG ondersteunt apparaten van de klant die verbinding maken via TLS 1.2.

UKG maakt gebruik van SFTP-services (Secure File Transfer Protocol), die met behulp van het Secure Shell Transfer-protocol een generiek eindpunt creëren voor bestandsuitwisseling met UKG Pro Workforce Management. Daarnaast wordt standaard PGP-bestandsencryptie toegepast bij alle integraties op bestandsbasis.

Data in rust: UKG biedt beveiliging op opslagniveau voor de data op het Google Cloud Platform voor productie- en niet-productieomgevingen van de klant. Hierbij wordt 256-bits AES-encryptie toegepast.

Klantdata worden streng beveiligd met encryptieprotocollen en cryptografie.

Netwerkbeveiliging

Alle internetverbindingen lopen via redundante firewalls om de toegang te controleren en het dataverkeer te monitoren en te loggen. UKG configureert de firewallregels zodanig dat dataverkeer standaard wordt geweigerd, tenzij er expliciet toestemming is verleend ('default deny'). De benodigde poorten en protocollen worden geopend op basis van specifieke doelen. Netwerkproxy's verbieden al het onnodige applicatieverkeer.

Er worden systemen voor inbraakdetectie en -preventie (IDS en IPS) toegepast om de risico's van inbraken en aanvallen door kwaadaardige software te beperken. Er worden kwetsbaarheidsscans uitgevoerd op de gehoste omgeving en de applicaties. Naar aanleiding van de uitkomsten van deze scans worden eventuele kwetsbaarheden verholpen volgens de specificaties in het SOC 2-rapport voor UKG.

Elektronische bestandsoverdracht tussen de cloudomgeving en de klant is toegestaan via SFTP of API's. Hardening-instellingen op productieservers worden gemonitord aan de hand van hardening-standaarden.

Toegangsbeheer voor applicaties

UKG Pro Workforce Management maakt gebruik van een multi-tenant implementatiestrategie waarbij de klantdata per databaseschema worden gescheiden. De toegang van tenants wordt beheerd via een beveiligde API-gateway en de resolutie van het dataverkeer vindt plaats aan de hand van de tenant-ID.

Het toegangsbeheer voor gebruikers van het UKG Pro Workforce Management-systeem wordt geregeld via configureerbare toegangsprofielen. Via twee soorten toegangsprofielen kunt u bepalen wat een gebruiker mag zien en mag doen, zodat u de toegang tot het systeem nauwkeurig kunt regelen aan de hand van de specifieke functievereisten van uw bedrijf:

Functietoegangsprofielen: Deze profielen bepalen welke functies een gebruiker in het systeem kan uitvoeren en wat de gebruiker mag doen.

Gegevenstoegang- en weergaveprofielen: Deze profielen bepalen niet alleen welke betalingscodes, werkregels en rapporten iemand in het systeem mag gebruiken, maar ook de weergave-instellingen die bepalen hoe een gebruiker de onderdelen van UKG Pro Workforce Management te zien krijgt. Via deze profielen wordt ook geregeld tot welke werknemers een manager toegang heeft.

Authenticatie

UKG Pro Workforce Management gebruikt het industriestandaard protocol SAML 2.0 voor SSO-integratie.

De authenticatieservice van UKG Pro Workforce Management ondersteunt een hoog-beschikbare federatieve SSO-service waarmee gebruikers bij UKG Pro Workforce Management kunnen inloggen vanaf zakelijke desktops, privécomputers voor thuiswerken en mobiele apparaten.

Voor klanten die niet naar SSO zijn gemigreerd, verzorgt de authenticatieservice van UKG Pro Workforce Management ook de basisauthenticatie. De gebruikersnamen en wachtwoorden worden in het UKG Pro Workforce Management-systeem opgeslagen voor klanten die de basisauthenticatie gebruiken. Klanten kunnen ervoor kiezen om sommige gebruikers (bijvoorbeeld managers) gebruik te laten maken van SSO en anderen van basisauthenticatie.

Toegangsbeheer en authenticatie

Het toegangsbeheer voor gebruikers van UKG Pro Workforce Management wordt geregeld via configureerbare toegangsprofielen. De authenticatie vindt plaats door middel van single sign-on (SSO).

Schaalbaarheid

UKG Pro Workforce Management heeft een gedistribueerde service-architectuur en maakt gebruik van microservices in een gelaagd platform.

UKG Pro Workforce Management biedt functionaliteit voor automatisering en cloudbeheer om de onderliggende infrastructuur van de softwareoplossing beschikbaar te stellen en te configureren. Hierdoor kunt u services horizontaal en/of verticaal onafhankelijk van elkaar op- en afschalen op basis van het werkelijke of verwachte gebruik.

UKG verzamelt een grote hoeveelheid infrastructuur- en applicatiestatistieken om de totale vraag naar services en de status en de prestaties van de omgeving te beoordelen. Deze statistieken worden zowel passief als actief gebruikt voor verschillende operationele doeleinden.

UKG past regelmatig cloudbeheer toe op basis van kwantitatieve en kwalitatieve gegevens uit de monitoring. De services worden op- of afgeschaald op basis van de werkelijke of verwachte belasting van het systeem.

Prestaties

UKG Pro Workforce Management ondergaat tijdens de ontwikkeling een rigoureuze evaluatie van de prestaties. Hierbij worden industriestandaard drempelwaarden gehanteerd voor interactief dataverkeer, integratieverkeer (API's) en achtergrondberekeningen en analyses. De oplossing is ontworpen en gebouwd voor krachtige prestaties om te voldoen aan de bedrijfsbehoeften van onze klanten in alle sectoren, ongeacht de werklast. Dit prestatie-evaluatieproces is ingebed in de levenscyclus van de softwareontwikkeling en geldt voor zowel nieuwe als bestaande capaciteiten.

In de klantgerichte omgevingen worden de responstijden regelmatig gemonitord met een combinatie van synthetische transactiemonitoring vanaf meerdere geografische locaties (representatief voor de klantervaring van het klantenbestand) en interne monitoring (representatief voor het UKG-gedeelte van de ervaring).

Interne tools voor prestatiemonitoring van applicaties bieden zichtbaarheid vanaf de rand van het UKG cloudnetwerk tot in de datalaag, zodat de specialisten van UKG eventuele prestatieproblemen nauwkeurig kunnen lokaliseren. De geaggregeerde gegevens uit de monitoringtools worden regelmatig geanalyseerd door speciale engineering- en onderhoudsteams om te zorgen dat UKG Pro Workforce Management ruimschoots voldoet aan de verwachtingen van onze klanten en onze eigen, strenge prestatie-eisen.

Prestatie-evaluatie

UKG Pro Workforce Management ondergaat tijdens de ontwikkeling een rigoureuze evaluatie van de prestaties. De oplossing is ontworpen en gebouwd voor krachtige prestaties om te voldoen aan de bedrijfsbehoeften van onze klanten in alle sectoren, ongeacht de werklast.

Hoge beschikbaarheid

De architectuur van UKG Pro Workforce Management heeft hoge beschikbaarheid en veerkracht ingebouwd in alle applicatielagen, zodat de 99,75% beschikbaarheid in de SLA wordt gehaald. Alle servicecomponenten op de web-, applicatie- en middleware-lagen zijn redundant uitgevoerd via mirroring over meerdere serverinstanties. Met load-balancing en softwareclustering wordt de beschikbaarheid verder geoptimaliseerd.

UKG Pro Workforce Management werkt met best-in-breed microservices om een werkelijk gedistribueerd platform te creëren dat hoge beschikbaarheid garandeert. Deze services maken een betere isolatie van storingen mogelijk: als één microservice uitvalt, blijven de andere gewoon werken. UKG kan meer services toevoegen en die services kunnen over meerdere nodes of zelfs datacenters worden gespreid als de vraag toeneemt.

Alle UKG Pro Workforce Management-databases maken gebruik van databaseclustering met synchrone of asynchrone streaming-replicatie tussen databaseservers en Google-zones.

Beschikbaarheid van de service

De services van UKG Pro Workforce Management zijn ontworpen om gebruik te maken van meerdere clouddatacenters (zones) binnen een geografisch gebied (regio). Mocht de service worden onderbroken, dan geldt een Recovery Time Objective (RTO) van 24 uur en een Recovery Point Objective (RPO) van 4 uur.

Calamiteitenherstel

Het speciale UKG Cloud Disaster Recovery Program zorgt dat het UKG Business Continuity Management Program voortdurend wordt nageleefd. In dit laatste programma zijn de vereisten voor de calamiteitenherstelplannen en crisisbeheerstrategieën van UKG vastgelegd.

De services van UKG Pro Workforce Management zijn ontworpen om gebruik te maken van meerdere clouddatacenters (zones) binnen een geografisch gebied (regio). Het UKG Cloud Disaster Recovery Program is gebaseerd op een alles-of-niets failover-strategie. Indien de UKG Pro Workforce Management-services van een klant vanwege een calamiteit niet beschikbaar zijn en niet binnen een aanvaardbare termijn hersteld kunnen worden, wordt de hele stack overgeschakeld naar de DR-regio.

Zodra de diensten in de DR-regio met succes zijn hersteld, fungeert die omgeving voortaan als productieregio. Om de continuïteit van de calamiteitenherstelservice van UKG Pro Workforce Management te handhaven, zal UKG vervolgens een nieuwe DR-regio inrichten als onderdeel van het failover-proces.

De Recovery Time Objective (RTO) is 24 uur en de Recovery Point Objective (RPO) is 4 uur.

Ultramoderne datacenters

UKG Pro Workforce Management wordt geïmplementeerd op het Google Cloud Platform (GCP). Beveiliging en gegevensbescherming staan voorop bij de ontwerpcriteria en maken integraal deel uit van alle processen van Google. De fysieke beveiliging van alle Google-datacenters bestaat uit een gelaagd beveiligingsmodel met beveiligingsmaatregelen zoals alarmsystemen, toegangsbarrières voor voertuigen, omheiningen, metaaldetectoren en biometrie. De datacenters van Google worden 24/7 bewaakt met hoge-resolutie binnen- en buitencamera's.

In de ruimtes dichter bij de servervloer van het datacentrum gelden extra verscherpte veiligheidsmaatregelen. Minder dan 1% van alle Google-werknemers zal ooit een voet in een Google-datacenter zetten. Uitsluitend bevoegde Google-werknemers met een specifieke taak mogen de servervloer betreden. Toegang tot de servervloer is alleen mogelijk via een beveiligingscorridor die is beveiligd met multi-factor toegangsbeheer op basis van badges en biometrische scans.

De Google Cloud draait op een technologieplatform dat bedacht, ontworpen en gebouwd is voor maximale veiligheid. Google is een vernieuwer in technologieën voor hardware, software, netwerken en systeembeheer. Op basis van deze deskundigheid heeft Google zijn servers, besturingssystemen en geografisch verspreide datacenters ontworpen volgens de principes van 'verdediging in de diepte'. Dit heeft geleid tot een IT-infrastructuur die veiliger en gemakkelijker te beheren is dan meer traditionele technologieën.

Het concept ‘verdediging in de diepte’ beschrijft meerdere verdedigingslinies die het netwerk van Google beschermen tegen aanvallen van buitenaf. Alleen geautoriseerde services en protocollen die aan alle veiligheidseisen van Google voldoen, worden toegelaten op het netwerk. Al het andere verkeer wordt automatisch genegeerd. Netwerken worden gescheiden door middel van industriestandaard firewalls en toegangscontrolelijsten. Al het verkeer wordt langs speciale GFE-servers (Google Front End) geleid om kwaadaardige verzoeken en DDoS-aanvallen op te sporen en tegen te houden. Bovendien mogen GFE-servers intern alleen communiceren met een gecontroleerde lijst van servers. Deze ‘default deny’- configuratie verhindert dat GFE-servers verbinding maken met ongewenste bronnen. Logboeken worden routinematig onderzocht om eventuele programmeerfouten aan het licht te brengen. Uitsluitend bevoegd personeel krijgt toegang tot de netwerkapparatuur.

De datacenters van Google zijn voorzien van redundante stroomvoorzieningen en klimaatbeheersingssystemen. Elk bedrijfskritisch onderdeel heeft een primaire en een alternatieve stroomvoorziening, beide met dezelfde capaciteit. Dieselaggregaten kunnen voldoende elektrische noodstroom leveren om alle datacenters op volle capaciteit te laten draaien.

Koelsystemen houden de bedrijfstemperatuur van servers en andere hardware constant, waardoor het risico van serviceonderbrekingen wordt verkleind.

Door middel van branddetectie- en -bestrijdingssystemen wordt schade aan hardware voorkomen. Hitte-, brand- en rookdetectoren genereren hoorbare en zichtbare alarmen in de betrokken ruimtes, op veiligheidsconsoles en in regelkamers op afstand.

The Google Cloud

Google is een vernieuwer in technologieën voor hardware, software, netwerken en systeembeheer. De Google Cloud draait op een technologieplatform dat bedacht, ontworpen en gebouwd is voor maximale veiligheid.

Systeemmonitoring en kwetsbaarhedenbeheer

UKG maakt gebruik van meerdere beveiligingslagen, te beginnen bij de netwerkperimeter, met geavanceerde firewalls, inbraakpreventiesystemen (IPS), inbraakdetectiesystemen (IDS), logboekmonitoring en antivirussoftware. De omgeving wordt voortdurend gemonitord.

De informatiesystemen voor beveiliging en eventmanagement gebruiken een combinatie van gegevensbronnen (app-, firewall- en IDS-logboeken) voor gedetailleerde analyse en het genereren van waarschuwingen. Naast de gegenereerde IDS-waarschuwingen is er een beveiligingsdashboard dat monitoring en analyse door de beveiligingsspecialisten van UKG vereenvoudigt. Op meerdere lagen worden detectie- en preventiemaatregelen toegepast.

Opslagsystemen

Google monitort de locatie en de status van alle opslagsystemen in de datacenters. Google past ook upgrades toe op verouderde hardware om de verwerkingssnelheid, de energie-efficiëntie en/of de opslagcapaciteit te optimaliseren.

Mediasanering en gegevensvernietiging

Google monitort de locatie en de status van alle opslagsystemen in de datacenters, van aankoop en installatie tot en met buitengebruikstelling en vernietiging, aan de hand van assetlabels die worden bijgehouden in de assetdatabase van Google. Fysieke opslagmedia kunnen om verschillende redenen buiten gebruik worden gesteld. Als een component op enig moment tijdens de levenscyclus niet slaagt voor een prestatietest, wordt deze buiten gebruik gesteld en ontmanteld. Google past ook upgrades toe op verouderde hardware om de verwerkingssnelheid, de energie-efficiëntie en/of de opslagcapaciteit te optimaliseren.

Altijd worden strikte voorzorgsmaatregelen in acht genomen, of opslagmedia nu vanwege een defect, een upgrade of om een andere reden buiten gebruik worden gesteld. Doordat de schijfeenheden van Google worden beveiligd met complete harddisk-encryptie, zijn de data ook tijdens de ontmanteling in rust beschermd. Bij elke ontmanteling van een harde schijf zorgen hiertoe bevoegde personen ofwel: 1) dat de schijf gegarandeerd gewist wordt door de hele schijf met nullen te overschrijven en daarna te verifiëren dat de schijf geen gegevens meer bevat; of 2) dat de schijf met behulp van speciaal gereedschap wordt geplet en vervormd of door een shredder wordt gehaald.

Over UKG

Bij UKG staan mensen centraal. Wij geloven met heel ons hart dat cultuur en saamhorigheid de sleutel tot succes is. Door fantastische werkplekken te bevorderen en levenslange partnerships op te bouwen met onze klanten laten we zien wat er mogelijk is als organisaties investeren in hun mensen. Met onze Life-work Technology-benadering van HR-, salaris- en workforce management oplossingen kunnen meer dan 75.000 organisaties in elke branche over de hele wereld de behoeftes van hun werknemers anticiperen en zich daaraan aanpassen.

Ga voor meer informatie over een van 's werelds toonaangevende HCM-cloudbedrijven naaf **ukg.nl**.

Our purpose is people