thinkproject!

SECURITYCONCEPT

Maatregelen voor het garanderen van de beschikbaarheid, vertrouwelijkheid en integriteit van data

- Hosting vanuit state-of-the-art, professioneel beheerde datacenters
- Apparatuur van hoge kwaliteit
- Naadloze monitoring en 24x7 service
- Maatregelen om ongeautoriseerde toegang tegen te gaan (wachtwoorden, twee-factor-authenticatie en/of IP-beperking optioneel)
- Veilige, gecodeerde dataoverdracht
- Controles ter bescherming tegen aanvallen van derden en malware
- Volledig redundante computers, Storage Area Network (SAN) en essentiële componenten van hoge kwaliteit
- Multi-level-back-up (gespiegelde datacenters, gespiegelde hoofdopslag, gespiegelde back-upopslag)
- Activiteiten conform Duitse wet inzake gegevensbescherming
- Gecertificeerde softwareontwikkeling, -implementatie en -activiteiten conform de internationale standaard voor informatiebescherming ISO/IEC 27001:2013

thinkproject!

HOSTING IN VEILIGE DATACENTERS

De think project!-cloud wordt beheerd vanuit twee aparte ISO/IEC 27001-gecertificeerde datacenters. Beide datacenters werken op basis van een 'active-active' benadering. In andere woorden: de verschillende elementen van onze dienstverlening draaien in beide datacenters om de workload evenredig te verdelen. Tegelijkertijd dient elk datacenter als back-up voor de ander. Doordat hun infrastructuur en hardware identiek zijn én dankzij volledig gespiegelde data kunnen beide datacenters binnen een paar minuten de taken van de ander overnemen. Dat betekent een continue bedrijfsvoering, zelfs in de ergst denkbare scenario's zoals fysieke uitval van een van de datacenters. Beide locaties zijn beveiligd via multi-level-toegangscontrolemechanismen en worden 24 uur per dag in de gaten gehouden.

State-of-the-art, professioneel beheerde datacenters

- Securitypersoneel aanwezig, 24 uur per dag, 365 dagen per jaar
- 7-level-toegangscontrolesysteem
- Permanente videomonitoring
- Hosting in gescheiden hardwarekasten, alleen toegankelijk voor geautoriseerd personeel
- Zeer goede internetverbinding met hoge bandbreedte
- Redundantie op basis van verschillende carriers
- Betrouwbare stroomtoevoer via redundante verbindingen met het elektriciteitsnet
- Noodstroom via UPS- en dieselgeneratoren
- Drie afzonderlijke brandalarmsystemen, brandbestendige muren en deuren
- Continue monitoring van temperatuur en luchtvochtigheid
- Gebruik van zeer precieze klimaatapparatuur
- 2-level-luchtfiltering

State-of-the-art apparatuur

Bij het selecteren van onze contractpartners voor netwerkinfrastructuur en hardware kiezen we uitsluitend voor toonaangevende leveranciers van bewezen oplossingen. Zo vertrouwen we onze netwerken en security toe aan Cisco en Juniper, en opslag aan EMC. De hardware van onze servers wordt geleverd door Fujitsu Technology Solutions.

Naadloze monitoring

De onderliggende serversystemen van de think project!-cloud zijn ontworpen voor maximale prestaties en beveiliging. De server-farm wordt naadloos gemonitord door een uitgebreide set tools. Deze security-tools controleren afzonderlijke parameters binnen systemen en toegankelijkheid van buitenaf. Op basis van hoe kritiek een vastgestelde gebeurtenis is, wordt een vooraf ingesteld alarmplan geactiveerd. Om storingen zo snel mogelijk te verhelpen – ook wanneer dit buiten de standaardkantooruren gebeurt – zijn onze technische medewerkers 24 uur per dag bereikbaar, zeven dagen per week.

UITGEBREIDE SECURITY-CONTROLE

Bescherming tegen ongeautoriseerde toegang

Toegang na invoeren wachtwoord: om toegang te krijgen tot de think project!-cloud hebben gebruikers login-gegevens nodig. Voor toegang tot een bepaald project is bovendien toestemming nodig van de projecteigenaar (de klant). Wachtwoorden worden encrypted opgeslagen. We bewaren enkel een 'digitale vingerafdruk' van elk wachtwoord. Deze procedure maakt het traceren van het origineel vrijwel onmogelijk. Zelfs onze eigen medewerkers kennen de gebruikerswachtwoorden niet. Uiteraard dient elke gebruiker zijn wachtwoord te beveiligen om ongeautoriseerd gebruik te voorkomen.

IP-beperking (optioneel): de think project!-cloud is via een internetverbinding vanaf vrijwel elke plek toegankelijk. Indien nodig kan toegang beperkt worden tot bepaalde bedrijfsnetwerken (zoals alleen het hoofdkantoor en uw bouwplaatskantoor). Dit wordt bewerkstelligd door het relevante IP-adres of adressen te specificeren en alle andere adressen te blokkeren.

Twee-factor-authenticatie (optioneel): voor twee-factor-toegangsbeveiliging maakt think project! gebruik van een oplossing van RSA Security, een toonaangevende internationale provider van authenticatietechnologie. Met deze methode dienen gebruikers in te loggen met een pincode van vier tot acht cijfers, gevolgd door een zescijferige pincode die op dat moment getoond wordt via een token. De SecurID-token genereert elke zestig seconden automatisch een nieuw zescijferig nummer.

Veilige dataoverdracht

Tenzij specifieke maatregelen geïmplementeerd zijn, wordt alle data op het internet overgedragen als platte tekst. Daardoor is data bij de overdracht van de ene naar de andere computer, eenvoudig te lezen, verwijderen of zelfs te veranderen. Om dit te voorkomen maken wij gebruik van encryptieprocedures die zorgen voor veilige dataoverdracht. Dat maakt blootstelling van data praktisch onmogelijk.

Bescherming tegen externe aanvallen

Om ons te beschermen tegen externe aanvallen, hanteren we de nieuwste multi-level-securitysystemen. Onze maatregelen bestaan onder andere uit:

- Dubbele firewall-systemen, te vergelijken met een dikke dubbele muur
- Scheiding tussen front- en backends, waardoor toegang van buitenaf alleen mogelijk is via een enkele 'security-poort', waarbij het gedeelte achter deze deur volledig afgesloten is
- Fysieke scheiding van applicatieservers en dataservers – applicaties draaien op de ene set, klantdata wordt opgeslagen op de andere

CONFORMITEIT MET DE HOOGSTE SECURITYSTANDAARDEN

Controles tegen malware

De verspreiding van malware, zoals computervirussen, wormen of Trojaanse paarden, is helaas aan de orde van de dag. We hebben speciale softwareprogramma's geïntegreerd die op een betrouwbare manier beveiligen tegen malware. Deze applicaties worden automatische meerdere keren per dag geüpdatet. Daardoor zijn nieuwe vormen en mutaties van malware direct te ontdekken. Dat een bestand dat malware bevat zich binnen think project! verspreidt, is daardoor vrijwel onmogelijk.

Veiligheidsmaatregelen tegen dataverlies

Redundante hardware: van de krachtige computers zijn identieke vervangingen beschikbaar, maar ook van de andere essentiële componenten zoals adapters, netwerkkaarten, harde schrijven en processors.
Volledig redundante Storage Area Network (SAN): ons SAN bestaat uit een serie hoogwaardige harde schijven die via glasvezel met elkaar verbonden zijn. In elk datacenter zijn identieke SAN-systemen geïnstalleerd, en in beide kan zo'n 350 terabyte aan niet-gecomprimeerde data worden opgeslagen. Voor extra beveiliging wordt alle data ook gespiegeld tussen de datacenters, zodat alle klantdata tweemaal wordt opgeslagen.
Externe opslag van back-updata: naast de data-back-up in onze gespiegelde Storage Area Networks, kopiëren we dagelijks alle data naar externe dataopslagmedia. De data wordt gesynchroniseerd met een tweede locatie binnen het back-upsysteem.

Activiteiten conform databeschermingswetgeving

think project! verzamelt, verwerkt, bewaart en gebruikt persoonlijke gegevens op basis van toegewezen dataverwerking overeenkomstig de Duitse wet voor gegevensbescherming (§ 11 BDSG). De zeggenschap over de organisatie en informatie blijft bij de klant.
Onze datacenters zijn gesitueerd in Duitsland en draaien daar ook. Data wordt binnen de Duitse landsgrenzen verwerkt en opgeslagen. think project!-werknemers zijn verplicht zich te houden aan gegevensbescherming volgens de Duitse wet gegevensbescherming (§ 5 BDSG) en om vertrouwelijkheid van telecommunicatie te handhaven volgens de Duitse Telemedia-wet (§ 88 TMG). Werknemers die een sleutelpositie innemen, zijn daarnaast in het bezit van een beveiligingsvergunning, overeenkomstig de Duitse veiligheidswet (SÜG).

Werkzaamheden en ontwikkeling conform internationale informatiebeveiligingsstandaarden

Onze beveiligingsstandaarden voor softwareontwikkeling en -implementatie zijn net zo hoog als die voor onze werkzaamheden. Softwareupdates worden eens per maand aangeleverd en afgerond. Deze updates bestaan uit correcties en nieuwe functies. Alle updates worden getest en goedgekeurd door ons kwaliteitsteam. De softwaretests worden uitgevoerd door state-of-the-art testautomationtools en worden ook handmatig uitgevoerd. De handmatige tests worden uitgevoerd volgens standaardprocedures zodat er niets over het hoofd wordt gezien. Grote aanpassingen, zoals verbeteringen in de gebruikersinterface, worden extra getest op een zogenaamd 'staging platform' waarop geselecteerde klanten, met name gebruikers die veel van het platform gebruikmaken, de nieuwe versie een laatste keer grondig testen. Updates worden pas geïmplementeerd wanneer deze tests succesvol zijn volbracht.


Certificate

Standard: ISO/IEC 27001:2013

Certificate Holder: think project! GmbH
Zamdorfer Str. 100
81677 München
Germany

including the location
think project! International GmbH & Co. KG
Eichenstr. 3b
12435 Berlin
Germany

Scope: Operation of the think project! cross-enterprise collaboration cloud, Professional Services, Product Management and Product Development of the think project! software including Quality Management, Marketing of the cross-enterprise collaboration solution think project!, Administration and Finance.

Proof has been furnished by means of an audit that the requirements of ISO/IEC 27001:2013 are met.

Validity: The certificate is valid from 2017-02-11 until 2020-02-10. First certification 2014

2017-03-22

www.tuv.com

TÜVRheinland® Precisely Right.

INTERNATIONALE INFORMATIEBEVEILIGINGSSTANDAARDEN

Het succes van ons bedrijf, alsook dat van onze klanten, is in hoge mate afhankelijk van toegankelijke informatie en efficiënte dataverwerking. Garantie van vertrouwelijkheid, beschikbaarheid en volledigheid van data is een must. Daarom is informatiebeveiliging een wezenlijk onderdeel van onze bedrijfsstrategie. Het door think project! geïmplementeerde Information Security Management System (ISMS) beslaat alle producten, diensten en bedrijfsprocessen, en is gecertificeerd volgens de internationale standaard ISO/IEC 27001:2013

TÜVRheinland ZERTIFIZIERT
Management System ISO 27001:2013
www.tuv.com ID 0024070852

thinkproject!

50 verschillende landen

10.000 projecten

› 150.000 gebruikers

Over think project!

Wereldwijd staat de bouwbranche voor vele uitdagingen. De druk om projecten op tijd en binnen budget op te leveren bijvoorbeeld, en de steeds groter wordende hoeveelheid data van een steeds groter aantal partijen die betrokken zijn bij bouw- en constructieprojecten.

Daardoor is er steeds meer behoefte aan digitale bouwoplossingen voor het bevorderen van samenwerking tussen meerdere organisaties en informatiemanagement in het algemeen. Oplossingen zoals think project!.

Met geavanceerde softwareoplossingen en branchedeskundig advies en diensten richt think project! zich op de moderne uitdagingen van digitalisering in de bouw en constructie.

think project! – uw partner voor digitale transformatie

Vertegenwoordigers wereldwijd
www.thinkproject.com/contact-us