thinkproject!

50 pays

10,000 projets

› 150,000 utilisateurs

A propos de think project!

Les enjeux du secteur de la construction au niveau mondial sont nombreux, notamment les impératifs de livraison des projets dans les délais et selon les budgets convenus, et le volume croissant d'informations générées par la multiplication des parties prenantes dans l'univers de l'ingénierie et du BTP.

De ce fait, on constate l'apparition d'une demande croissante pour des solutions de construction digitales comme celles de think project! qui facilitent la collaboration transversale inter-entreprises et la gestion globale des informations.

think project! répond aux enjeux actuels de la digitalisation dans l'ingénierie et la construction avec des solutions logicielles à la pointe de la technologie, et son expertise en conseil et services pour les professionnels du secteur.

think project! – votre partenaire pour la transformation digitale

Les représentants à travers le monde
www.thinkproject.com/contact-us

thinkproject!

CONCEPT DE SECURITE

Mesures prises pour garantir la disponibilité, la confidentialité et l'intégrité des données

- Hébergement dans un centre de données à la pointe des technologies et du professionnalisme
- Equipements de haute performance
- Suivi 24h/24 sans interruption 7 jours par semaine
- Mise en place de mesures de protection contre l'accès non autorisé (mots de passe, option d'authentification à deux facteurs et/ou restriction selon IP)
- Transfert de données sécurisé par cryptage
- Contrôles de protection contre les intrusions frauduleuses et malware (les logiciels malveillants)
- Parc informatique entièrement redondant de haute performance, y compris le SAN (réseau de stockage) et les composants essentiels
- Sauvegardes à de multiples niveaux (centres de données mise en miroir, stockage principal miroir, stockage de sauvegardes en miroir)
- Opérations conformes à la législation allemande en matière de protection des données
- Edition de logiciel certifiée, déploiements et activités conformes à la norme internationale de sécurité ISO/IEC 27001:2013

thinkproject.com

HÉBERGEMENT DANS DES CENTRES DE DONNÉES SÉCURISÉS

Le cloud (serveur distant) de think project! se situe dans deux centres de données distincts certifiés ISO/IEC 27001 exploités en mode „actif-actif“. Autrement dit, différentes parties de nos services se déploient dans l'un ou l'autre de ces centres en vue d'une répartition équilibrée de la charge. Ainsi chaque centre de données sert en même temps d'auxiliaire à l'autre. Grâce à leurs infrastructures et équipements identiques, et au système en miroir appliqué à toutes les données, il suffit de quelques minutes pour que l'un des centres de données assume la charge de l'autre. Ceci garantit une exploitation continue même dans un scénario de crise majeure, par exemple la perte physique de l'un ou l'autre des centres. Les deux sites sont protégés par des contrôles d'accès à multiples niveaux, et placés sous surveillance permanente 24 heures sur 24.

Des centres de données à la pointe de la technologie et du professionnalisme

- Protégés par des équipes de sécurité sur le site 24 heures par jour, 365 jours par an
- Un système de contrôle d'accès à sept niveaux
- Surveillance vidéo permanente
- Hébergement dans des baies informatiques séparées, accessibles uniquement au personnel autorisé
- Connexion internet ultra-rapide avec larges bandes pas santes haut débit
- Redondance à multi-porteurs
- Reliés en permanence au réseau électrique grâce aux connexions redondées
- Courant d'urgence en permanence via UPS et des groupes électrogènes
- 3 systèmes différents d'alarme incendie, murs anti-incendie et portes coupe-feu
- Contrôle en continu de la température et de l'humidité ambiantes
- Dispositifs de climatisation de précision
- Filtrage de l'air à 2 niveaux

Equipements à la pointe de la technologie

Pour construire l'infrastructure de notre réseau et choisir nos équipements informatiques, nous retenons exclusivement pour partenaires contractuels des fournisseurs leaders sur le marché. Nous confions la fourniture du réseau et la sécurité aux sociétés Cisco et Juniper, tandis que le stockage est géré par EMC. Nos serveurs et équipements informatiques sont fournis par Fujitsu Technology Solutions.

Surveillance en mode continu

La ferme de serveurs qui assure le cloud de think project! est conçue pour assurer performance et sécurité maximales. Elle fait l'objet d'une surveillance en continu par un ensemble d'outils complet. Ces outils de sécurité vérifient sans cesse tant les différents paramètres au sein des systèmes que leur accessibilité depuis l'extérieur. En fonction du niveau de criticité des incidents identifiés, le système déclenche un plan d'alerte préprogrammé. Afin de remédier aux dysfonctionnements le plus rapidement possible — y compris en dehors des heures de travail — notre équipe technique intervient 24h sur 24, sept jours par semaine.

UN ENSEMBLE COMPLET DE DISPOSITIFS DE SÉCURITÉ

Protection contre l'accès non autorisé

Accès protégé par des mots de passe: L'accès au cloud de think project! requiert un mot de passe de tout utilisateur. L'accès à un projet spécifique nécessite en outre l'autorisation du maître d'ouvrage (client). Ces mots de passe ne sont pas stockés en mode lisible, chacun étant enregistré au moyen d'une „empreinte numérique“ rendant pratiquement impossible le traçage de son original. Cette procédure signifie qu'aucun de nos collaborateurs ne connaît véritablement ses mots de passe. Naturellement, chaque utilisateur devra veiller à la sécurité de son mot de passe pour le préserver d'une utilisation par des tiers non autorisés.
En option : restriction selon IP: L'accès au cloud de think project! peut se faire partout au moyen d'une connexion internet. Le cas échéant, l'accès peut être restreint aux réseaux internes (par ex., depuis votre siège ou votre bureau sur un chantier). Il suffit pour cela d'indiquer la ou les adresses IP autorisées et de bloquer toutes autres adresses.
En option : authentification à deux facteurs: Pour notre dispositif d'accès à deux facteurs, nous mettons en œuvre une solution développée par RSA Security, l'un des premiers fournisseurs mondiaux dans le secteur de la technologie d'authentification. Avec cette méthode, les utilisateurs tapent de leur code PIN de quatre à huit chiffres , suivis d'un code d'autorisation à six chiffres qui à ce moment-là apparaît sur l'écran sous la forme d'un jeton. Le jeton de sécurité SecurID génère un nouveau code à six chiffres sur l'écran toutes les 60 secondes.

Transfert de données sécurisé

Sauf mise en œuvre de précautions particulières, toutes les données transmises via l'internet apparaissent en mode texte, et de ce fait sont relativement faciles à lire, à supprimer voire à altérer lors de leur transfert d'un ordinateur à l'autre. Afin d'empêcher de telles manipulations, nous procédons à un cryptage des données qui permet de sécuriser leur transmission, réduisant à quasiment zéro leur exposition au risque.

Protection contre l'intrusion de tiers

Nous recourons aux systèmes de sécurité les plus récents et à niveaux multiples afin de protéger nos réseaux contre le risque d'intrusions frauduleuses, notamment:

- Systèmes de double pare-feu, comparable à un mur épais et doublé
- Une séparation entre l'entrée et la sortie, ce qui se traduit par l'impossibilité d'y accéder autrement que par une „porte de sécurité“ unique assurant une isolation complète
- La séparation physique des serveurs d'application de ceux qui traitent les données, ce qui permet la mise en œuvre des applications sur un corps de systèmes, et le stockage des données clients sur l'autre.

Contrôles contre les logiciels malveillants

La propagation de logiciels malveillants (malware) via des virus ou des chevaux de Troie fait malheureusement partie de la vie quotidienne. Nous travaillons avec des logiciels dédiés qui protègent efficacement contre ces « maliciels », avec des applications de mises à jour automatiques multiples dans une même journée permettant d'identifier aussitôt les maliciels dans leurs nouvelles formes et mutations. Ainsi, au sein de think project!, le traitement et la dissémination d'un fichier infecté par un logiciel malveillant est quasiment impossible.

Mesures de prévention contre la perte de données

Equipements informatiques redondants: Les ordinateurs à haute performance sont tous dupliqués, à l'identique, toujours disponibles, tout comme d'autres éléments essentiels tels les adaptateurs, les cartes de réseau, les disques durs et les processeurs.
Réseau de stockage (SAN) entièrement redondant: Notre SAN (storage area network, ou réseau de stockage de données) comprend une série de disque durs de grande qualité reliés par des câbles en fibre optique. Chacun de nos centres de données est équipé de systèmes SAN identiques, d'une capacité de stockage unitaire d'environ 350 terabytes de données non compressées. Pour renforcer encore la
sécurité, toutes ces données sont mises en miroir dans les deux centres de données, ce qui équivaut à une double sauvegarde de toutes les données de nos clients.
Données sauvegardées en stockage externe: En complément à notre sauvegarde de données SAN mises en miroir, nous copions quotidiennement la totalité des données dans des supports de mémoire externes. Les données sont synchronisées dans un deuxième local au sein du système de sauvegarde.

CONFORMITÉ AUX NORMES DE SÉCURITÉ LES PLUS STRICTES

Opérations en conformité avec la législation relative à la protection des données

think project! recourt à des prestataires de services pour la collecte, le traitement, le stockage et l'utilisation de données personnelles, à des conditions conformes à la loi allemande sur la protection des données (§ 11 BDSG). Le client conserve la maîtrise en matière de l'organisation et l'information.
Nos centres de données étant situés et exploités en Allemagne, les données seront traitées et stockées sur le territoire allemand. Les collaborateurs de think project! ont l'obligation de se conformer à la loi allemande sur la protection des données (§ 5 BDSG), et de préserver la confidentialité des télécommunications conformément à la loi allemande Telemedia (§ 88 TMG). En outre, les personnes clés au sein de la société ont fait l'objet d'une habilitation en sécurité selon la législation allemande en matière de sécurité (SÜG).

Fonctionnement et développement conformes aux normes de sécurité internationales

Les normes de sécurité que nous appliquons dans l'édition et le déploiement de nos logiciels sont aussi strictes que celles mises en œuvre pour nos activités. Les logiciels sont mis à jour en continu avec de nouvelles versions livrées chaque mois, comportant des corrections et de nouveaux éléments fonctionnels. Toutes les mises à jour sont testées et avalisées par notre équipe de contrôle qualité, au moyen d'outils automatisés et par des tests manuels, pour ceux-ci effectués selon des protocoles standardisés, pour garantir que rien ne passe inaperçu. Les modifications majeures, par exemple au niveau de l'interface de l'utilisateur, font l'objet d'une vérification supplémentaire sur une „staging platform“, soit une plateforme de simulation où des clients sélectionnés selon un critère d'habitude de fréquentation assidue soumettent les nouveautés à une dernière épreuve complète. Les mises à jour ne sont déployées qu'après réussite de tous les essais.


Certificate

Standard: ISO/IEC 27001:2013
Certificate Registr. No.: 01 153 1302603
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.

LES NORMES INTERNATIONALES DE SÉCURITÉ DES INFORMATIONS

La réussite de nos activités, comme celle de nos clients, dépend en grande partie de l'accès aux informations et d'un traitement efficace des données. Il est primordial d'assurer la confidentialité, la disponibilité et l'intégrité des informations à tout moment. Ainsi, la sécurité des informations fait partie intégrante de notre stratégie. Le système de gestion de leur sécurité (Information Security Management System, ou l'ISMS) mis en œuvre par think project! s'étend à l'ensemble de nos produits, services et processus. Il est certifié par le label ISO/IEC 27001:2013.

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