Foire aux questions sur la police de protection des données de Joineer AG

Nous sommes heureux de répondre comme suit aux questions les plus fréquemment posées en matière de sécurité :

1. Comment l'authentification est-elle résolue, comment un(e) employé(e) peut-il/elle se connecter ?

Le client enregistre les employé(e)s participant(e)s dans le fichier Excel fourni par Joineer avec leur prénom, nom, adresse e-mail et affiliation à une équipe. Pour les administrateurs d'équipe ou d'entreprise, cela est noté en conséquence. En outre, la hiérarchie et les questions sont enregistrées dans un processus itératif avec Joineer dans le même fichier Excel. Les employé(e)s ne s'inscrivent pas réellement via le système, mais sont enregistré(e)s à l'avance. Le matin du début de l'enquête, les employé(e)s participant(e)s recevront un e-mail automatisé de l'expéditeur no-reply@app.joineer.com via mg.joineer.ch. Dans cet e-mail, les participant(e)s sont informé(e)s de l'enquête et se rendent dans notre système app.joineer.com avec le lien de connexion personnalisé (via un bouton dans l'e-mail). Si l'employé(e) n'a pas été saisi(e) dans Excel, il/elle ne recevra pas de lien de connexion et sans lien, il/elle ne pourra pas accéder au système.

Après un formulaire de consentement, les participant(e)s sont dirigé(e)s vers l'enquête. Les réponses quantitatives et qualitatives sont protégées lors de la saisie par la connexion cryptée du protocole de transmission hypertexte sécurisé. Consultez les documents relatifs à la politique de confidentialité et à l'architecture informatique pour savoir comment l'application web et la base de données sont protégées.

2. Votre solution prend-elle en charge le SSO / 2FA ?

Après s'être connectés au système, les participant(e)s peuvent configurer un accès protégé par mot de passe à l'outil au lieu d'un accès direct via le lien reçu par e-mail. Les participant(e)s accèdent à cette option via le tableau de bord (Dashboard) → Profil → Activer la protection par mot de passe. Désormais, les participant(e)s qui ont activé la protection par mot de passe se connectent au système via l'URL https://app.joineer.com/ avec leur e-mail et leur mot de passe. Pour le stockage, le salage et hachage des mots de passe sont utilisés.

Cette procédure d'authentification unique est basée sur des algorithmes de cryptage et des méthodes d'authentification actuels et sécurisés. Les données sensibles sont cryptées à sens unique et ne peuvent donc pas être lues par les administrateurs de Joineer AG. Elles sont

protégées par un cryptage SSL (Secure Sockets Layer). Grâce à des sauvegardes quotidiennes et à plusieurs disques durs en miroir, nous garantissons une sécurité maximale pour les données.

Pour des besoins de sécurité accrus, nous proposons une authentification à deux facteurs, par laquelle chaque participant(e) saisit son numéro de téléphone mobile après avoir rempli l'enquête, afin d'accéder ultérieurement aux résultats de l'enquête à l'aide d'un code.

3. Comment l'accès sécurisé au tableau de bord est-il assuré ?

La première façon d'accéder au tableau de bord est d'utiliser l'e-mail de lancement de l'enquête. Dans cet e-mail, les participant(e)s sont informé(e)s de l'enquête et peuvent accéder à notre application app.joineer.com avec le lien de connexion personnalisé (via un bouton dans l'e-mail). Les personnes qui n'ont pas été saisies dans Excel ne recevront pas de lien de connexion et sans lien, elles ne pourront pas accéder au système. Après avoir saisi les réponses quantitatives et qualitatives, les participant(e)s sont redirigés vers le tableau de bord. Si aucune enquête n'est en cours, les participant(e)s sont directement dirigés vers le tableau de bord via le lien figurant dans l'e-mail de résultats automatisé. Si le/la participant(e) a activé la protection par mot de passe, il/elle sera dirigé vers l'écran de connexion via l'URL https://app.joineer.com/, où il/elle pourra se connecter au système avec son adresse e-mail et son mot de passe. Après s'être connecté(e), le/la participant(e) est dirigé(e) vers le tableau de bord. Ici aussi, toutes les activités sont protégées par la connexion cryptée du protocole de transmission hypertexte sécurisé.

Si l'authentification à deux facteurs est paramétrée, l'accès n'est possible que par une double authentification via le téléphone mobile. Dès que l'utilisateur souhaite consulter les résultats ou modifier un paramètre du système, il devra confirmer son identité grâce à un code envoyé par SMS.

4. Les données sensibles sont-elles cryptées ? (Pour le transfert comme pour le stockage)

Toutes les données de la base de données Mongo DB sont stockées dans un centre de données de première qualité certifié ISO9001 et ISO27001 en Suisse, qui est protégé 24 heures sur 24 et 7 jours sur 7 par du personnel de sécurité contre les accès physiques non autorisés et les pannes majeures. ISO/IEC 27001 est la norme la plus connue en matière de sécurité de l'information, qui impose des exigences élevées à un Système de Gestion de la Sécurité de l'Information (SGSI). Le centre de données suisse répond aux exigences des normes FINMA-RS 08/7 et 18/3.

Ansible est utilisé comme outil pour assurer une configuration uniforme (règles de pare-feu, désactivation des services inutiles). Le système d'exploitation est Ubuntu LTS (Long Term Support), qui est particulièrement adapté à une utilisation sur serveur.

Chaque version LTS est prise en charge pendant au moins 5 ans après sa sortie (mises à jour de sécurité). L'accès de gestion à la machine physique n'est possible qu'à partir du réseau de gestion spécifique (aucune exposition à l'Internet). Vous trouverez plus d'informations à ce sujet dans le document Architecture informatique et protection des données de Joineer AG.

Les données sont sécurisées lors du transfert via le protocole de transfert hypertexte sécurisé. Si nécessaire, nous pouvons transmettre l'ensemble des données au client sous forme cryptée et lui fournir la clé correspondante. Les données brutes sensibles, que nous ne sommes pas autorisés à décrypter en raison du RGPD (GDPR), n'en font pas partie. Il ne doit pas être possible de tirer des conclusions sur les réponses de personnes individuelles. Pour ce transfert de données, nous pouvons proposer un cryptage par "clé à usage unique" et vous envoyer la clé, par exemple par téléphone portable/SMS.

5. Les clés de chiffrement sont-elles également accessibles au client ?

Nous ne fournissons pas de clés à un client pour accéder au serveur. Comme mentionné ci-dessus, nous pouvons transmettre l'ensemble des données sous forme cryptée si le client le demande et fournir la clé correspondante. Les données brutes sensibles, que nous ne sommes pas autorisés à décrypter en raison du RGPD (GDPR), n'en font pas partie. Il ne doit pas être possible de tirer des conclusions sur les réponses de personnes individuelles. Pour ce transfert de données, nous pouvons proposer un cryptage par "clé à usage unique" et vous envoyer la clé, par exemple par téléphone portable/SMS.

6. Existe-t-il une documentation technique pour votre solution système ?

Oui, vous pouvez trouver notre documentation technique dans le document **Architecture informatique.**