FAQ sull’informativa della privacy di Joineer AG

Siamo felici di rispondere alle domande più frequenti relative alla sicurezza nel modo seguente:

1. Come viene risolta l'autenticazione, in che modo un dipendente può effettuare l'accesso?

Il cliente inserisce i dati dei dipendenti partecipanti in un file Excel fornito da Joineer: esso contiene il loro nome, cognome, indirizzo email e appartenenza al team di lavoro. Sia i capo reparto che gli amministratori aziendali vengono registrati di conseguenza. Inoltre, la gerarchia e le domande sono registrate nello stesso file Excel in un processo iterativo insieme a Joineer. I dipendenti non si registrano effettivamente attraverso il sistema, ma vengono registrati in anticipo. La mattina dell'inizio del sondaggio, i dipendenti partecipanti ricevono un'e-mail automatica dal mittente no-reply@app.joineer.com via mg.joineer.ch. In questa e-mail, i partecipanti vengono informati sia sulle domande, sulla gerarchia e anche che il link d’accesso personalizzato serve ad accedere al sistema app.joineer.com (tramite pulsante nell'e-mail). Se il dipendente non è stato inserito in Excel, non riceverà un link di accesso e senza un link non si può accedere al sistema. Dopo una dichiarazione di consenso, i partecipanti vengono condotti al sondaggio. Le risposte quantitative e qualitative sono protette durante l'inserimento grazie alla trasmissione criptata del protocollo di trasmissione ipertestuale sicuro. Vedi la politica sulla privacy e i documenti sull'architettura IT per informazioni su come l'applicazione web e il database sono protetti.

2. La vostra soluzione supporta SSO / 2FA?

Non appena i partecipanti avranno effettuato l'accesso al sistema, potranno impostare l'accesso protetto da password per il tool invece dell'accesso diretto tramite il link dell'email. I partecipanti accedono a questa opzione tramite Dashboard → Profilo → Abilita protezione con password. D'ora in poi, i partecipanti che avranno attivato la protezione con password potranno accedere al sistema tramite l'URL https://app.joineer.com/ con il loro indirizzo e-mail e la loro password. Le password di accesso sono esclusivamente “salted” e sottoposte a hashing. Questa procedura di single sign-on è basata su algoritmi di crittografia e metodi di autenticazione attuali e sicuri. I dati critici per la sicurezza sono criptati a senso unico e quindi non possono essere letti dagli amministratori di Joineer AG e sono protetti dalla crittografia SSL. Backup quotidiani e dischi rigidi ridondanti e con mirroring garantiscono la massima sicurezza dei dati.

In caso di maggiori esigenze di sicurezza, offriamo un'autenticazione a due fattori (2FA), in cui ogni partecipante inserisce il suo numero di cellulare dopo aver completato il sondaggio per poter accedere ai risultati del sondaggio in un secondo momento utilizzando un codice.

3. Come viene garantito l'accesso sicuro al dashboard?

Il primo modo per accedere al dashboard è tramite l'e-mail con cui si dà inizio al sondaggio. In questa e-mail, i partecipanti sono informati sul sondaggio e possono accedere al nostro sistema app.joineer.com con il link di accesso personalizzato (tramite un pulsante nella e-mail). Coloro che non sono stati inseriti nel foglio Excel non riceveranno un link di accesso e senza un link non potranno accedere al sistema. Dopo aver inserito le risposte quantitative e qualitative, i partecipanti vengono reindirizzati al dashboard. Se nessun sondaggio è in corso, i partecipanti vengono condotti direttamente alla dashboard tramite il link nell'e-mail per visualizzare i risultati. Se il partecipante ha attivato la protezione con password, sarà indirizzato alla schermata di accesso tramite l'URL https://app.joineer.com/, dove potrà accedere al sistema con il suo indirizzo e-mail e la sua password. Dopo aver effettuato il login, il partecipante viene indirizzato al dashboard. Anche qui, tutte le attività sono protette dalla connessione criptata con il protocollo di trasmissione ipertestuale sicuro.

Se l'autenticazione a due fattori è impostata, l'accesso è possibile solo tramite doppia autenticazione via cellulare. Non appena l'utente vorrà visualizzare i risultati nel sistema o cambiare un'impostazione, dovrà autenticarsi tramite un codice SMS.

4. I dati sensibili sono criptati? (per il trasferimento e lo stoccaggio)

Tutti i dati nel database Mongo DB sono memorizzati in un centro dati di prima classe certificato ISO9001 e ISO27001 in Svizzera, il quale è protetto 24 ore su 24 (7 giorni su 7) da personale addetto alla sicurezza per evitare accessi fisici non autorizzati e guasti gravi. ISO/IEC 27001 è lo standard più noto in materia di sicurezza delle informazioni, e pone alti requisiti a un sistema di gestione della sicurezza delle informazioni (ISMS). Il centro dati svizzero soddisfa i requisiti della FINMA-RS 08/7 e 18/3.

Ansible è usato come strumento di gestione della configurazione per assicurare una configurazione uniforme (regole del firewall, disattivazione dei servizi non necessari). Il sistema operativo utilizzato è Ubuntu LTS (Long Term Support), che è particolarmente adatto all'uso come server. Ogni release LTS è supportato per almeno 5 anni dopo il suo rilascio.

(Aggiornamenti di sicurezza). L'accesso alla gestione della macchina fisica è possibile solo dalla rete di gestione apposita (nessuna esposizione a Internet). Ulteriori informazioni possono essere trovate nel documento Architettura IT e protezione dei dati Joineer AG.

I dati sono protetti durante la trasmissione tramite il protocollo di trasmissione ipertestuale sicuro. Se necessario, possiamo trasmettere tutti i dati al cliente in forma criptata e fornire la chiave corrispondente. I dati grezzi sensibili, che non siamo autorizzati a decifrare a causa del DSGOV (GDPR), non rientrano in tale contesto. Non deve essere possibile trarre conclusioni sulle risposte

delle singole persone. Per questo dump di dati, possiamo offrire una crittografia "one-time key" e inviare la chiave per esempio tramite cellulare/SMS.

5. Le chiavi di criptazione sono accessibili anche al cliente?

Non forniamo chiavi a nessun cliente per accedere al server. Come menzionato in precedenza, possiamo trasmettere tutti i dati in forma criptata se richiesto dal cliente e fornire la chiave corrispondente. I dati grezzi sensibili, che non siamo autorizzati a decifrare a causa del DSGOV (GDPR), non rientrano in tale contesto. Non deve essere possibile trarre conclusioni sulle risposte delle singole persone. Per questo dump di dati, possiamo offrire una crittografia "one-time key" e inviarvi la chiave, ad esempio per telefono cellulare/SMS.

6. Esiste una documentazione tecnica per la vostra soluzione di sistema?

Sì, potete trovare la nostra documentazione tecnica nel documento Architettura IT.