CORPORATE TRAVELLER™ | Propulsé par melon

Sécurité des renseignements (InfoSec) Fiche de données

Protection des renseignements

- Infrastructure partagée
  - Conforme aux normes PCI-DSS et RGPD
- Cycle de vie de développement système (SDLC) conçu sur la base de ces normes et cadres :
  - RGPD
  - Adhésion au cadre de sécurité et de confidentialité dès la conception de Flight Centre Travel Group (FCTG, société mère de Corporate Traveler)
  - Projet ouvert de sécurité des applications Web (OWASP)
  - ISO 27001
- Bases de sécurité minimales définies à l'aide du CIS et du NIST et révisées chaque année.
- Toutes les données chiffrées au repos à l'aide d'AES356 et en cours de transport à l'aide de TLS 1.2.
- Les données des clients ne peuvent pas être stockées sur l'équipement des employés.
- McAfee ePO et Microsoft Defender utilisés pour la protection contre les logiciels malveillants et les virus sur tous les points finaux et serveurs.
- Gestion des vulnérabilités assurée par Tenable, protection contre les activités malveillantes via SIEM et SOC complets 24h/24, 7j/7 et 365j/an et tests d'intrusion par Trustwave Dvuln ou Bugcrowd
- Tous les développeurs utilisent Snyk et résolvent les vulnérabilités trouvées dans le code.

Audits de systèmes TI

- Analyses de vulnérabilités externes effectuées mensuellement
  - Trustwave pour les sites Web réseau et externes (Internet)
  - Verizon (QSA) effectue régulièrement des évaluations de sécurité par des tiers
- Résultats examinés et mesures correctives menées à l'interne par la haute direction de l'informatique et de la sécurité, conformément aux politiques de sécurité internes.

Contrôle des accès

- Corporate Traveller dispose d'un processus d'autorisation, de provisionnement et de désapprovisionnement de l'accès des employés clients.
- Possibilité d'intégration à votre système RH via un flux de données de routine, y compris les avis de licenciement.
- La plateforme Corporate Traveller Melon offre un accès à une authentification unique dans lequel Corporate Traveller peut s'intégrer à l'authentification conforme SAML 2.0 existante des clients pour supprimer la nécessité pour Corporate Traveller d'enregistrer les mots de passe des utilisateurs ou les informations de connexion.

- Les employés en voyage d'affaires s'authentifient via des connexions sécurisées, notamment un VPN basé sur un certificat à deux facteurs pour un accès multifacteur (MFA), des connexions basées sur SSL et une authentification basée sur Windows.
- Examens trimestriels des droits d'accès des utilisateurs

Mots de passe

- Les premiers mots de passe pour les nouveaux utilisateurs et les mots de passe réinitialisés pour les utilisateurs existants sont définis sur une valeur unique pour chaque utilisateur et modifiés après la première utilisation.
- Les mots de passe sont stockés sous forme de hachage bcrypt dans le texte postgres
- Les mots de passe des comptes d'utilisateurs doivent respecter les normes minimales suivantes (peuvent être augmentées en fonction des spécifications du client) :
  - Une longueur de mot de passe d'au moins 7 pour les comptes d'utilisateurs, la politique indiquant 12
  - Exigences de complexité conformes aux normes PCI-DSS
  - Les mots de passe doivent être modifiés régulièrement – 90 jours
  - Les mots de passe ne peuvent pas être identiques au dernier mot de passe
  - L'accès au compte est temporairement suspendu après 5 tentatives en 30 minutes
- Les fonctionnalités de délai d'inactivité des sessions de bureau ont été définies sur 15 minutes ou moins. L'inactivité de la session du processeur expire après 30 minutes
- Tous les accès à distance protégés par MFA

Stockage de données, contrôles physiques et reprise après sinistre

- Les centres de données FCTG se trouvent sur la plate-forme cloud Microsoft Azure et sont physiquement situés en Virginie, aux États-Unis. Microsoft Azure est conforme aux normes de l'industrie telles que ISO 27001, ISO 27018, ISO 9001, ISO 22301, HIPAA, FedRAMP, PCI DSS, SSAE-18 SOC 1 et SOC 2 pour la sécurité logique et physique, l'intégrité du traitement et la disponibilité. Concur et Sabre sont également conformes à SOC 2.
- Microsoft Azure s'exécute dans des installations Microsoft géographiquement réparties, partageant l'espace et les utilitaires avec d'autres services en ligne Microsoft. Chaque installation est conçue pour fonctionner 24 heures sur 24, 7 jours sur 7, 365 jours par an et utilise diverses mesures pour aider à protéger les opérations contre les pannes de courant, les intrusions physiques et les pannes de réseau. Des sauvegardes sont effectuées régulièrement pour éviter la perte de données client par Azure.
- Données de rapports téléchargées sur ClientBank, l'environnement PowerBI de Corporate Traveller, où les données sont entièrement cryptées et gérées par FCTG.

Ressources humaines

- Vérifications d'antécédents effectuées au Canada, notamment :
  - Vérification et traçabilité du numéro NAS
  - Records provinciaux
  - Vérification de l'éducation
- Programme de formation de sensibilisation à la sécurité requis pour tous les nouveaux employés et répété chaque année

Gestion des incidents

- La surveillance de la sécurité est effectuée via une solution Global SIEM qui surveille les serveurs clés et l'infrastructure réseau. Les incidents peuvent être suivis jusqu'à des utilisateurs spécifiques, des modifications de fichiers et de serveurs. Les gestionnaires d'incidents, les analystes de la sécurité de l'information et le centre des opérations de sécurité évalueront les événements de sécurité pour déterminer la gravité et la voie de remontée appropriée, et effectueront des analyses médico-légales et des causes profondes appropriées pour identifier, suivre et résoudre les incidents de sécurité.