Computershare

NOUS PROTÉGEONS VOS DONNÉES:

Sécurité de l'information chez Computershare

Avril 2024

Lors du choix d'un partenaire pour gérer certaines parties de votre entreprise, de nombreux facteurs tels que l'expertise, la qualité du service et les coûts de la technologie jouent un rôle. L'un des facteurs les plus importants de ce partenaire est le niveau de sécurité de l'information.

Computershare, en tant que leader mondial de services financiers, prend la sécurité de vos données aussi au sérieux que vous. Reconnus par plus de 40'000 clients représentant des millions d'ensembles de données de parties prenantes, les meilleures précautions possibles sont prises pour protéger les données qui nous sont confiées. Nous gérons chaque année 850 assemblées en Europe continentale et 7'500 assemblées dans le monde entier, les données des assemblées et des actionnaires étant protégées en toute sécurité dans nos systèmes.

Sécurité des informations – cadre général

En tant que fournisseur de services mondial, nos procédures d'information et de cybersécurité répondent aux exigences régionales des juridictions dans lesquelles nos clients sont actifs.

En conséquence, nos procédures sont stables, continuellement testées, développées et contrôlées par une équipe interne d'experts en sécurité de l'information.

Notre cadre général mondial pour l'information et la cybersécurité est conforme aux normes ISO/IEC 27002:2013, normes internationales qui comprendent des recommandations pour divers mécanismes de contrôle de la sécurité de l'information.

Nos cadres générales en Allemagne sont également conformes aux normes ISO 27001, ISO 9001 et sont conformes à TISAX (AL2) et confirmées par l'association ENX.

Ce cadre général, qui couvre toutes les activités et sites de Computershare, y compris l'Europe, vise l'objectif suivant:

- Évaluation régulière des cyber-risques et menaces, protection des données clients hautement sensibles contre les failles de sécurité, les accès non autorisés, les infections par des logiciels malveillants et les attaques DDoS (Distributed Denial of Service).
- Conformité aux réglementations légales dans le monde entier. Le règlement général de l'UE sur la protection des données (RGPD), le changement le plus important apporté à la législation sur la protection des données au cours des 20 dernières années, permet aux individus plus de contrôle et de droits sur leurs données personnelles. Les systèmes de Computershare sont conformes au RGPD et disposent de contrôles pour sauvegarder et assurer la sécurité des données personnelles afin qu'elles puissent être traitées conformément à ces exigences.

Nos politiques et cadres de gestion des risques, conformes aux directives ISO 31000, contrôlent de manière cohérente les mesures de gestion des risques dans tous les secteurs d'activité.

Ce cadre général soutient les objectifs de Computershare en matière de risque en fournissant une approche cohérente pour identifier, analyser, atténuer et rapporter les risques et les contrôles dans des niveaux de tolérance acceptables.

Nos cadres d'information ainsi que de cybersécurité et de gestion des risques sont examinés par les divisions commerciales et technologiques de Computershare et approuvés par notre conseil d'administration.

Infrastructure de sécurité de l'information

Notre réseau informatique et les technologies de support (passerelles de réseau, commutateurs, routeurs, firewalls, serveurs et terminaux) sont gérés et contrôlés par le groupe Technology Services de Computershare.

Les contrôles techniques de sécurité comprennent les principes de l'architecture de sécurité (c.-à-d. Defense-in-Depth, Least Privilege, Default Deny et Fail Secure) et les directives de renforcement de la sécurité (c.-à-d. l'utilisation de protocoles de cryptage sécurisés et la désactivation des protocoles/versions non sécurisés).

Notre méthodologie de Defense-in-Depth utilise différentes technologies et emplacements pour atténuer les effets d'une attaque DDoS ou SYN/FLOOD. Nous utilisons plusieurs fournisseurs de services internet pour réduire la surface d'attaque grâce à diverses options de basculement, ainsi que d'autres solutions et dispositifs de surveillance pour une protection supplémentaire.

Nous disposons de solides journaux de surveillance et d'alerte au niveau du réseau, des applications et des serveurs afin de suivre les performances de notre système en temps réel. Des plans de réponse aux incidents, y compris des procédures spécifiques pour les attaques DDoS, sont en place pour permettre la détection, le confinement, l'élimination et la récupération des telles attaques.

Programmes de sécurité de l'information

Lorsqu'il s'agit de maintenir l'information et la cybersécurité, le champ d'application est vaste. De nombreux scénarios doivent être envisagés pour protéger la confidentialité des données des clients et des informations des actionnaires.

Les programmes que nous avons mis en place pour assurer et surveiller en permanence notre périmètre de sécurité comprennent:

- Gestion et classification des données
- Surveillance du système et du réseau
- Inventaire et gestion des dispositifs
- Développement de systèmes et d'applications et l'assurance qualité
- Contrôles d'accès et gestion des identités
- Sécurité physique et contrôles environnementaux
- Plan de continuité des activités et de reprise après sinistre
- Protection des données clients
- Fonctionnement et disponibilité du système
- Évaluations des risques des fournisseurs et des tiers
- Gestion de la sécurité du système et du réseau
- Gestion des incidents

Sécurité des informations 24 x 7 x 365

Le risque de cyberattaques est toujours là. Computershare est toujours vigilant. Nous examinons de manière proactive les menaces émergentes, les tendances et les exigences réglementaires croissantes.

Notre Security Operations Center centralisé surveille, analyse et réagit 24 heures sur 24 aux événements suspects. Computershare fait appel à des parties internes et externes pour surveiller activement l'environnement des menaces internes et externes et pour tester la sécurité des applications et de l'infrastructure sous-jacente.

Des contrôles de sécurité réguliers sont effectués afin de valider et de suivre les menaces de manière indépendante. Si des problèmes techniques potentiels sont identifiés lors des tests, les mesures correctives et de contrôle nécessaires sont prises. Un rapport est établi à l'intention de la direction.

Pour les applications critiques, des tests complets sont effectués chaque année par des sociétés externes. Nous commandons également plusieurs audits externes afin de faire vérifier et confirmer de manière indépendante nos contrôles commerciaux et technologiques.

Ces audits externes comprennent les contrôles des systèmes et de l'organisation (SOC), International Standard on Assurance Engagements (ISAE) 3402, Statement on Standards for Attestation Engagements (SSAE) 18, Australian Standard on Assurance Engagements (ASAE) 3150 et ISO 27001:2013, qui s'appliquent à certaines unités commerciales et sites.

Des équipes de sécurité de l'information **dédiées**, expérimentées et qualifiées dans le monde entier

27'000+

de nos principaux comptes système sont protégés par notre outil de gestion des mots de passe à l'échelle de l'entreprise

Classement de sécurité

"advanced"

de Bitsight Technologies, le système de notation préféré de l'industrie

8'000+

heures consacrées par les collaborateurs de Computershare à des formations électroniques obligatoires sur la sécurité de l'information

2'000+

audits réalisés par les clients

3'500+

heures de piratage éthique et d'examen technique de nos propres systèmes

Analyses **quotidiennes** automatisées des vulnérabilités des réseaux de notre entreprise et des actifs internes

Security Operations Center

24 x 7

avec une couverture mondiale toute l'année

Plus de

0,8 million

de droits d'accès certifiés

Des millions

investis dans la sécurité de l'information chaque année