Computershare

WIR SCHÜTZEN IHRE DATEN:

Informationssicherheit bei Computershare

April 2024

Bei der Auswahl eines Partners, der Teilbereiche Ihres Geschäfts abwickeln soll, spielen viele Faktoren wie Expertise, Servicequalität, Technologie oder Kosten eine Rolle. Einer der wichtigsten Faktoren ist aber der Informationssicherheitsstandard des Partners.

Als weltweit führender Anbieter von Finanzdienstleistungen nehmen wir die Sicherheit Ihrer Daten genauso ernst wie Sie selbst. Unsere mehr als 40.000 Kunden weltweit und rund 300 deutschen Emittenten, die Millionen von Datensätzen halten, vertrauen darauf, dass wir die bestmöglichen Vorkehrungen treffen, um die uns anvertrauten Aktionärs-, Versammlungs- und Registerdaten sicher in unseren Systemen zu verwalten.

Informationssicherheit bei Computershare

Als globaler Dienstleister entsprechen unsere Informations- und Cybersicherheitsverfahren den regionalen Anforderungen der Länder, in denen unsere Kunden aktiv sind.

Dementsprechend sind unsere Verfahren robust, werden kontinuierlich getestet, weiterentwickelt und von einem internen Team von Informationssicherheitsexperten überwacht.

Unser globales Informations- und Cybersicherheits-Framework entspricht der ISO/IEC 27002:2013, einem internationalen Standard, der Empfehlungen für diverse Kontrollmechanismen für die Informationssicherheit beinhaltet.

Unser Framework in Deutschland entspricht darüber hinaus der ISO 27001, ISO 9001 und ist TISAX-konform (AL2), wie von der ENX Association bestätigt.

Diese Rahmenwerke, die alle Geschäftsbereiche und Standorte von Computershare inklusive Europa abdecken, dienen folgenden Zielen:

- Regelmäßige Evaluierung von Cyber-Risiken und -Bedrohungen und Schutz hochsensibler Kundendaten vor Sicherheitsverletzungen, unbefugtem Zugriff, Malware-Infektionen und DDoS-Angriffen (Distributed Denial of Service).
- Einhaltung gesetzlicher Vorschriften weltweit. Die EU-Datenschutzgrundverordnung (DSGVO), die größte Änderung im Datenschutzrecht der letzten 20 Jahre, gibt dem Einzelnen mehr Kontrolle und Rechte über seine persönlichen Daten. Die Systeme von Computershare sind DSGVO-konform und verfügen über Kontrollen, um die Sicherheit personenbezogener Daten zu gewährleisten und sicherzustellen, dass sie in Übereinstimmung mit den Anforderungen verarbeitet werden.

Unsere Risikomanagement-Richtlinie und unser Rahmenwerk, das der ISO 31000 entspricht, überwachen die Maßnahmen zum Risikomanagement einheitlich in allen Geschäftsbereichen.

Dieser Sicherheitsrahmen unterstützt die Risikoziele von Computershare, indem er einen einheitlichen Ansatz zur Identifizierung, Analyse, Milderung und Berichterstattung von Risiken und Kontrollen innerhalb akzeptabler Toleranzschwellen bietet.

Sowohl unser Informations- als auch unser Cybersicherheits- und Risikomanagement-Rahmen werden von unseren Geschäfts- und Technologiebereichen geprüft und von unserem Vorstand genehmigt.

Infrastruktur der Informationssicherheit

Unser IT-Netzwerk und die unterstützenden Technologien (Netzwerk-Gateways, Switches, Router, Firewalls, Server und Endgeräte) werden von der Computershare Technology Services Group betreut und kontrolliert.

Die technischen Sicherheitskontrollen umfassen die Grundsätze der Sicherheitsarchitektur (d. h. Defense-in-Depth, Least Privilege, Default Deny und Fail Secure) und Richtlinien zur Sicherheitssteigerung (d. h. Verwendung sicherer Verschlüsselungsprotokolle und Deaktivierung unsicherer Protokolle/Versionen).

Unsere Defense-in-Depth-Methode nutzt verschiedene Technologien und Einsatzorte, um die Auswirkungen eines DDoS- oder SYN/FLOOD-Angriffs abzuschwächen. Wir nutzen verschiedene Internet-Serviceprovider, um die Angriffsfläche durch verschiedene Failover-Optionen zu verkleinern, sowie weitere Lösungen zur Weiterleitung und Überwachung des Datenverkehrs für zusätzlichen Schutz.

Wir haben solide Überwachungs- und Warnprotokolle auf Netzwerk-, Anwendungs- und Serverebene, um unsere Systemleistung in Echtzeit zu verfolgen. Es gibt Pläne für die Reaktion auf Zwischenfälle, einschließlich spezieller Verfahren für DDoS-Angriffe, die die Erkennung, Eindämmung, Ausmerzung und Wiederherstellung nach solchen Angriffen ermöglichen.

Programme zur Informationssicherheit

Wenn es um die Aufrechterhaltung der Informations- und Cybersicherheit geht, ist die Bandbreite groß, und es müssen viele Szenarien berücksichtigt werden, um die Vertraulichkeit von Kundendaten und die Privatsphäre von Aktionärsinformationen zu schützen.

Die Programme, die wir zur kontinuierlichen Sicherung und Überwachung unserer Sicherheitslandschaft eingerichtet haben, umfassen:

- Datenmanagement und -klassifizierung
- System- und Netzwerküberwachung
- Bestandsaufnahme und Geräteverwaltung
- System- und Anwendungsentwicklung und Qualitätssicherung
- Zugangskontrollen und Identitätsmanagement
- Physische Sicherheit und Umgebungskontrollen
- Business Continuity- und Disaster Recovery-Pläne
- Schutz der Kundendaten
- Systembetrieb und Verfügbarkeit
- Risikobewertungen von Lieferanten und Drittanbietern
- System- und Netzwerksicherheitsmanagement
- Unmittelbare Reaktion auf Zwischenfälle

Informationssicherheit 24 x 7 x 365

Da die Gefahr von Cyberangriffen immer besteht, ist Computershare stets wachsam. Wir überprüfen proaktiv neu auftretende Bedrohungen, Trends und zunehmende regulatorische Anforderungen.

Unser zentralisiertes Security Operations Center überwacht, analysiert und reagiert rund um die Uhr auf verdächtige Ereignisse. Computershare setzt interne und externe Parteien ein, um das interne und externe Bedrohungsumfeld aktiv zu überwachen und die Sicherheitslage der Anwendungen sowie der zugrunde liegenden Infrastruktur zu testen.

Darüber hinaus führen wir regelmäßige Sicherheitskontrollen durch, um Bedrohungen unabhängig zu validieren und ihnen nachzugehen. Wenn potenzielle technische Probleme identifiziert werden, werden die erforderlichen Maßnahmen zur Beseitigung und Kontrolle ergriffen und es erfolgt ein Bericht an die Geschäftsleitung.

Penetrationstests durch externe Anbieter finden jährlich für kritische Anwendungen statt. Weiterhin geben wir externe Audits in Auftrag, um unsere Geschäfts- und Technologiekontrollen unabhängig prüfen und bestätigen zu lassen.

Diese externen Audits umfassen System- und Organisationskontrollen (SOC), International Standard on Assurance Engagements (ISAE) 3402, Statement on Standards for Attestation Engagements (SSAE) 18, Australian Standard on Assurance Engagements (ASAE) 3150 und ISO 27001:2013, die für bestimmte Geschäftsbereiche und Standorte gelten.

Dedizierte, erfahrene und qualifizierte InfoSec-Teams weltweit

27.000+
unserer wichtigsten Systemkonten werden durch unser unternehmensweites Passwort-Management-Tool geschützt

Sicherheitseinstufung
"advanced"
von Bitsight Technologies, dem bevorzugten Ratingsystem der Industrie

8.000+
Stunden, die unsere Mitarbeiter mit verpflichtenden e-Trainings zu Informationssicherheit verbracht haben

2.000+
kundenseitige Audits absolviert

3.500+
Stunden Ethical Hacking und technische Überprüfung unserer eigenen Systeme

Tägliche
automatisierte Schwachstellen-Scans unserer Firmennetzwerke

24 x 7
Security Operations Center mit ganzjähriger globaler Abdeckung

Über **0,8 Millionen**
Zugriffsberechtigungen zertifiziert

Millionen-
Investments in Informationssicherheit jedes Jahr