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 und Technologiekosten eine Rolle. Einer der wichtigsten Faktoren dieses Partners ist der Standard für Informationssicherheit.

Computershare, als weltweit führender Anbieter von Finanzdienstleistungen, nimmt die Sicherheit Ihrer Daten genauso ernst wie Sie. Mehr als 40‘000 Kunden, die Millionen von Stakeholder-Datensätzen repräsentieren, vertrauen darauf, dass bestmögliche Vorkehrungen getroffen werden, um die uns anvertrauten Daten zu schützen. Wir verwalten jährlich 850 Versammlungen in Kontinentaleuropa und 7‘500 Versammlungen weltweit, wobei die Versammlungs- und Aktionärsdaten in unseren Systemen sicher geschützt sind.

Informationssicherheit - Rahmenbedingungen

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

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

Unsere globalen Rahmenbedingungen für Informations- und Cybersicherheit entsprechen den Normen ISO/IEC 27002:2013, einem internationalen Standard, der Empfehlungen für diverse Kontrollmechanismen von Informationssicherheit beinhaltet.

Unsere Rahmenbedingungen in Deutschland entsprechen zudem den Normen ISO 27001, ISO 9001 und sind TISAX-konform (AL2) sowie von der ENX Association bestätigt.

Diese Rahmenbedingungen, die alle Geschäftsbereiche und Standorte von Computershare einschliesslich Europa abdecken, dienen folgendem Ziel:

- Regelmässige Evaluierung von Cyber-Risiken und -Bedrohungen, Schutz hochsensibler Kundendaten vor Sicherheitsverletzungen, unbefugtem Zugriff, Malware-Infektionen sowie DDoS-Angriffen (Distributed Denial of Service).
- Einhaltung gesetzlicher Vorschriften weltweit. Die EU-Datenschutz-Grundverordnung (DSGVO), die bedeutendste Änderung des Datenschutzrechts in den letzten 20 Jahren, ermöglicht dem Einzelnen mehr Kontrolle und Rechte über seine personenbezogenen Daten. Die Systeme von Computershare sind DSGVO-konform und verfügen über Kontrollen, um die Sicherheit personenbezogener Daten zu gewährleisten und stellen sicher, dass sie gemäss dieser Anforderungen verarbeitet werden können.

Unsere Risikomanagementrichtlinien und Rahmenbedingungen, die den Richtlinien ISO 31000 entsprechen, überwachen die Massnahmen zum Risikomanagement konsequent über alle Geschäftsbereiche hinweg.

Diese Rahmenbedingungen unterstützen die Risikoziele von Computershare, indem sie einen einheitlichen Ansatz zur Identifizierung, Analyse, Milderung und Berichterstattung von Risiken und Kontrollen innerhalb akzeptabler Toleranzschwellen bieten.

Sowohl unsere Informations- als auch unsere Cybersicherheits- und Risikomanagement-Rahmenbedingungen werden von den Geschäfts- und Technologiebereichen von Computershare überprüft und unserem Vorstand genehmigt.

Infrastruktur für Informationssicherheit

Unser IT-Netzwerk und die unterstützenden Technologien (Netzwerk-Gateways, Switches, Router, Firewalls, Server und Endgeräte) werden durch die Technology Services-Gruppe von Computershare 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-Methodik nutzt verschiedene Technologien und Einsatzorte, um die Auswirkungen eines DDoS- oder SYN/FLOOD-Angriffs abzuschwächen. Wir verwenden mehrere Internet-Dienstleister, um die Angriffsfläche durch verschiedene Ausfallschutzoptionen zu reduzieren, sowie andere Lösungen und Überwachungsgeräte für zusätzlichen Schutz.

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

Programme zur Informationssicherheit

Wenn es um die Aufrechterhaltung der Informations- und Cybersicherheit geht, ist der Anwendungsbereich breit gefächert. Viele Szenarien müssen berücksichtigt werden, um die Vertraulichkeit von Kundendaten und die Privatsphäre von Aktionärsinformationen zu schützen.

Die Programme, die wir zur kontinuierlichen Sicherung und Überwachung in unserem Sicherheitsbereich eingerichtet haben, umfassen:

- Datenmanagement und -klassifizierung
- System- und Netzwerküberwachung
- Bestandsaufnahme und Geräteverwaltung
- System-, Anwendungsentwicklung und Qualitätssicherung
- Zugangskontrollen und Identitätsmanagement
- Physische Sicherheit und Umgebungskontrollen
- Geschäftskontinuitäts- und Notfallwiederherstellungsplan
- Schutz der Kundendaten
- Systembetrieb und Verfügbarkeit
- Risikobewertungen von Lieferanten und Drittanbietern
- System- und Netzwerksicherheitsmanagement
- Verwaltung von Vorfällen

Informationssicherheit 24 x 7 x 365

Die Gefahr von Cyberangriffen besteht immer. Computershare ist 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 nutzt interne und externe Parteien, um die interne und externe Bedrohungsumgebung aktiv zu überwachen und die Sicherheit von Anwendungen sowie der zugrunde liegenden Infrastruktur zu testen.

Regelmässige Sicherheitskontrollen werden durchgeführt, um Bedrohungen unabhängig zu validieren und zu verfolgen. Sind potenzielle technische Probleme während der Tests identifiziert, werden die erforderlichen Massnahmen zur Beseitigung und Kontrolle ergriffen. Eine Berichterstattung an das Management erfolgt.

Für kritische Anwendungen finden jährlich umfassende Penetrationstest statt, die von externen Firmen durchgeführt werden. Wir geben auch mehrere 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.

Engagierte,
erfahrene und qualifizierte Informationssicherheitsteams weltweit

27'000+
unserer wichtigsten Systemkonten sind mit unserem unternehmensweiten Passwort-Management-Tool geschützt

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

8'000+
Stunden, die von Mitarbeitenden von Computershare für obligatorische E-Trainings zur Informationssicherheit aufgewendet wurden

2'000+
kundenseitige Audits absolviert

3'500+
Stunden Ethical Hacking und technische Überprüfung unserer eigenen Systeme

Tägliche
automatisierte Schwachstellenscans unserer Firmennetzwerke und internen Assets

24 x 7
Security Operations Center mit ganzjähriger globaler Abdeckung

Über **0,8 Millionen**
zertifizierte Zugriffsberechtigungen

Millionen
von Investitionen in Informationssicherheit jedes Jahr