Instone Group

Cybersecurity Policy

Cybersecurity Policy

Datenschutz- und Governance-Strukturen

- Ziel unserer IT-Sicherheitsstrategie ist es, den kontinuierlichen Betrieb der IT-Systeme sicherzustellen und unberechtigte Zugriffe auf unsere Systeme und Datenbanken zu verhindern.
- Wir haben eine Governance-Struktur mit klar definierten Rollen und Verantwortlichkeiten. Der IT-Leiter ist für die Erreichung der IT-Sicherheitsziele und der Sicherheitsgrundsätze Vertraulichkeit, Integrität und Verfügbarkeit verantwortlich. Er berichtet direkt an den CEO.
- Der für das konzernweite IT-Sicherheitsrisikomanagement und Datenschutzmaßnahmen zuständige Datenschutzbeauftragte unterstützt den IT-Leiter.
- Wir halten uns strikt an die geltenden Gesetze zum Schutz und zur Sicherheit personenbezogener Daten. Unsere IT-Landschaft und internen Prozesse wurden an diese Gesetze, d. h. die Datenschutz-Grundverordnung (DSGVO), angepasst.
- IT-Sicherheitsrisiken werden im allgemeinen Risikomanagementsystem des Konzerns laufend bewertet und gesteuert.
- Wir haben konzernweite Datenschutz- und Cybersicherheitsrichtlinien für alle Mitarbeiter veröffentlicht.
- Wir haben ein konzernweites Verzeichnis der Verarbeitungstätigkeiten sowie standardisierte Prozesse zur Überprüfung der Einhaltung der Datenschutzbestimmungen implementiert

Regelmäßige Mitarbeiterschulungen und Rechtemanagement

- Alle Mitarbeiter müssen sich in ihren Arbeitsverträgen zu Datenschutzrichtlinien verpflichten, um die Vertraulichkeit von Informationen zu gewährleisten.
- Wir führen jährlich obligatorische zertifizierte Datenschutzschulungen für alle Mitarbeiter durch. Darüber hinaus

schulen wir unsere Mitarbeiter regelmäßig per E-Mail zu Cybersecurity-Themen wie Phishing-Mails, Ransomware etc.
- Der Zugriff auf unsere Systeme ist eingeschränkt. Alle Mitarbeiter können nur auf die Daten zugreifen, die sie für ihre tägliche Arbeit benötigen.
- Der Zugriff auf unsere Systeme ist ebenfalls durch Zwei-Faktor-Authentifizierung gesichert
- Dienstleister: ISO 27001-Zertifizierung
- Unsere wichtigsten IT-Dienstleister sind nach ISO 27001 zertifiziert. Dies ist für eine Geschäftsbeziehung zwingend erforderlich.
- Darüber hinaus müssen unsere Dienstleister separate Sicherheitsrichtlinien, umfassende Service-Level-Agreements einschließlich Service-Level-Agreements zur Datenwiederherstellung akzeptieren und befolgen.

Operative Maßnahmen zur Überwachung und Reaktion auf Datenschutzverletzungen und Cyberangriffe

- Kontinuierliche Bedrohungsanalyse durch Analyse von BSI-Cert. Das Computer Emergency Response Team (CERT) des Bundesamtes für Sicherheit in der Informationstechnik erstellt und veröffentlicht unter anderem Empfehlungen für präventive Maßnahmen, weist auf Schwachstellen in Hard- und Softwareprodukten hin und schlägt Maßnahmen zur Behebung bekannter Schwachstellen vor.
- Unsere Systeme sind so ausgelegt, dass sie vor einem kompletten Systemausfall geschützt sind, um eine kontinuierliche Systemverfügbarkeit zu gewährleisten. Unsere gesamte Software wird regelmäßig aktualisiert, um Fehler zu beheben, potenzielle Sicherheitslücken zu schließen und die Funktionalität zu erhöhen. (Monatliche Aktualisierung aller Clients und Server, tägliche Aktualisierung des Client-Virenschutzes, tägliche Aktualisierung der Gruppennetzwerk-Firewall...).
- Nutzung eines externen professionellen Cloud Security Operation Center (CSOC): 24/7 automatische und manuelle Überwachung und ereignisgesteuerte aktive Durchführung von Cyber-Abwehrmaßnahmen, wie Sperrung von Konten und Abschaltung gefährdeter Netzwerkbereiche oder Server.

Regelmäßige interne und externe Präventionsmaßnahmen und Sicherheitsaudits

- Wir haben ein definiertes Verfahren zur Verwaltung von Software-Upgrades (Patch-Management) eingerichtet, um Risiken zu beherrschen, die durch veraltete Software oder durch Software-Upgrades entstehen können. Das Patch-Management wird intern und jährlich durch unseren externen Auditor engmaschig überwacht.
- Alle Systeme und Daten werden regelmäßig gesichert. Wir verwenden ausgelagerte Rechenzentren in Europa (Frankfurt und Amsterdam). Kritische Daten werden über Rechenzentren und Standorte hinweg repliziert. Darüber hinaus führen wir Datensicherungen auf Bändern durch.
- Um Datenverlusten vorzubeugen, führen wir regelmäßig Fehler- und Neustartübungen mit allen wichtigen Systemen durch.
- Zusätzlich setzen wir Microsoft Defender for Identity (ehemals Advanced Azure Information & Threat Protection / ATP) ein, eine cloudbasierte Sicherheitslösung inklusive Vorwarnfunktion bei verdächtigen Aktivitäten in unserem Netzwerk.
- Wir führen regelmäßig Sicherheits- und Penetrationstests sowie Cyber Risk Assessments mit externen Dienstleistern durch.
- Unsere externen Auditoren überprüfen jährlich unsere IT-Sicherheitsmaßnahmen und -prozesse, einschließlich Benutzerverwaltung (Anlegen, Löschen), Identitäts- und Zugriffsmanagement, Änderungsmanagement z.B. im SAP-System, Datenkonsistenz
- Jährlich werden interne Sicherheitsaudits durchgeführt