Überblick über die Sicherheit von Board Cloud

board

Inhalt

1. Einleitung

Dieses Dokument gibt einen Überblick über Compliance-Richtlinien, Zertifizierungen und unterstützende Prozesse, die Board anwendet, um die Daten in Board Cloud zu schützen und zu sichern.
Board International (im Folgenden "Das Unternehmen" oder "Board") verpflichtet sich, die Grundsätze der Vertraulichkeit, Integrität, Verfügbarkeit und des Vertrauens seiner Kunden zu erfüllen und dauerhaft aufrechtzuerhalten. Board ist sich bewusst, dass dies für die Geschäftstätigkeit seiner Kunden von grundlegender Bedeutung ist.

Board legt größten Wert darauf, Kundenbeziehungen aufzubauen, die auf gegenseitigem Vertrauen beruhen. Dazu schafft Board Transparenz über Abläufe, Richtlinien und Verfahren zum Schutz der Kundendaten.
Board verpflichtet sich, die Leistung dauerhaft zu sichern und sich an den höchsten Sicherheitsstandards messen zu lassen. Board analysiert kontinuierlich die aktuellen Bedrohungen und nutzt sie, um seine aktuellen Richtlinien und Verfahren zur Informationssicherheit als integralen Bestandteil seines Services zu verbessern.
Das leistungsstarke Sicherheitsprogramm von Board berücksichtigt sorgfältig die Aspekte des Datenschutzes in allen Bereichen des Serviceangebots für die Kunden.

2. Board Cloud – ein Überblick

Board Cloud ist eine Software as a Service (SaaS)-Version der Board All-in-One-Plattform und bietet erstklassige Sicherheit, Zuverlässigkeit, Skalierbarkeit und Leistung.

Board nutzt Microsoft Azure als IAAS-Anbieter für Board Cloud. Sicherheit ist ein wesentlicher Bestandteil bei Entwicklung, Tests und Bereitstellung des Produkts und des Cloud-Services durch Board.

Höchste Sicherheit wird durch verschiedene Methoden erreicht, die Aspekte wie Authentifizierung, Verschlüsselung, Schwachstellenüberwachung und zahlreiche andere Sicherheitstechnologien abdecken.

3. Board Software as a Service

3.1 Rechenzentren und Sicherheit

Board Cloud wird über die Rechenzentren von Microsoft Azure bereitgestellt. Die geografische Abdeckung von Microsoft Azure ermöglicht es, die verschiedenen lokalen Richtlinien und regulatorischen Anforderungen an die Verarbeitung und Speicherung personenbezogener Daten und Finanzdaten zu erfüllen, und so ein Höchstmaß an Sicherheit, Zuverlässigkeit, Transparenz und Compliance zu gewährleisten.

Alle Rechenzentren sind als ANSI/TIA-942 Tier 4, also der höchsten Stufe, klassifiziert und wurden von Grund auf für unternehmenskritische Computersysteme entwickelt. Sie werden mit vollständig redundanten Subsystemen für maximale Sicherheit betrieben. Die Partnerschaft mit Microsoft ermöglicht es, Board-Server in der Nähe der Rechenzentren des Kunden oder in der Nähe seiner User zu platzieren. Dadurch werden Latenzprobleme vermieden, die in globalen Implementierungen auftreten können.
Kunden können den für ihre Implementierung geeignetsten geografischen Standort aus den verfügbaren Microsoft-Rechenzentren auswählen.

Auf der Website **http://www.azurespeed.com/Information/AzureRegions** können Kunden den besten geografischen Standort ermitteln. Die Datenspeicherung kann auf ein einzelnes Land, eine Region oder ein geografisches Gebiet beschränkt werden **(siehe Abb. 1 - Microsoft Azure Regionen).**

Abb. 1 – Microsoft Azure Regionen

Microsoft wendet strenge Sicherheitskriterien an, die den Betrieb und den Support regeln. Microsoft setzt dabei eine Kombination von präventiven, defensiven und reaktiven Maßnahmen ein. Diese umfassen die folgenden Mechanismen zum Schutz vor unbefugten Entwickler- und/oder Administratoraktivitäten:

- **Strenge Zugriffskontrollen für sensible Daten, einschließlich einer Zwei-Faktor-Smartcard-basierten Authentifizierung zur Durchführung sensibler Vorgänge;**
- **Kombinationen von Maßnahmen, die eine unabhängige Erkennung von bösartigen Aktivitäten unterstützen;**
- **Mehrere Ebenen von Überwachung, Protokollierung und Reporting.**

Darüber hinaus führt Microsoft Hintergrundüberprüfungen für ausgewählte Mitarbeiter durch und beschränkt den Zugriff auf Anwendungen, Systeme und Netzwerkinfrastrukturen je nach Ergebnis der Hintergrundüberprüfung.

Microsoft Azure erfüllt eine breite Palette internationaler sowie regionaler und branchenspezifischer Compliance-Standards wie ISO 27001, FedRAMP, SOC 1 und SOC 2. Die Einhaltung der strengen Sicherheitsmaßnahmen, die diese Standards erfordern, wird durch genaue Audits von Drittanbietern überprüft, die belegen, dass die Azure-Services mit erstklassigen Industriestandards, Zertifizierungen, Bescheinigungen und Autorisierungen arbeiten und diese einhalten.

Weitere Informationen finden Sie unter
https://www.microsoft.com/en-us/trustcenter/compliance/complianceofferings?product=Azure.

Board nutzt die Vorteile der breiten Palette an Sicherheitswerkzeugen und -funktionen, um den Geschäftszielen zu entsprechen und Industriestandards und -vorschriften einzuhalten.

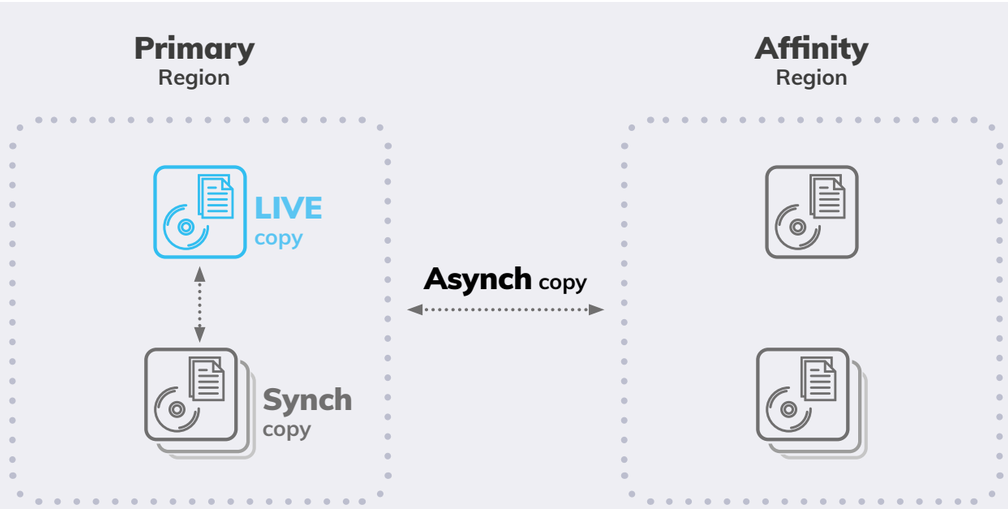
3.2 Service- und Datenredundanz

Die Datenspeicherung jedes Kunden ist lokal redundant und zusätzlich georedundant.

Die Geo-Redundanz basiert auf der Affinitätsregion (z.B. Central US, East US....).

Board Cloud bietet Kunden eine skalierbare und hoch belastbare Architektur. Um das zu gewährleisten, wird der Account synchron innerhalb der primären Region und asynchron zur sekundären Region repliziert. Das gewährleistet eine Datenverfügbarkeit von min. 99,99% (siehe Abb. **2 - Redundanz der Board Cloud**).

Abb. 2 – Redundanz der Board Cloud



Die Verfügbarkeit und Unversehrtheit der Daten und der Board-Services sind gewährleistet.

Board Cloud garantiert die folgenden Service Level Agreements (SLA) für die Reaktivierung des Services:

- **Das RTO (Recovery Time Objective), d.h. die Zeitspanne, in der die Verfügbarkeit der Board-Cloud-Services nach einer möglichen Unterbrechung oder Einschränkung wiederhergestellt wird, darf maximal 6 Stunden betragen;**
- **Das RPO (Recovery Point Objective), d.h. das maximale Zeitintervall, in dem Kundendaten aufgrund einer ungeplanten Unterbrechung oder Einschränkung von Board-Cloud-Services verloren gehen und wiederhergestellt werden, darf max. 1 Tag betragen.**

4. Datensicherheit

4.1 Kundendaten

Der Kunde ist alleiniger Eigentümer aller auf das System geladener Kundendaten.
Der Kunde hat alle Rechte, Ansprüche und Interessen an und auf alle seine Kundendaten.
Das Cloud Operation-Team hat nur in den folgenden beiden Szenarien Zugriff auf Kundendaten:

- **Mit vorheriger schriftlicher Zustimmung des Kunden, um auf systembedingte oder technische Probleme zu reagieren;**
- **Auf schriftliche Anfrage des Kunden in Übereinstimmung mit den schriftlichen Anweisungen des Kunden.**

4.2 Datenisolierung

Board Cloud bietet Kunden eine oder mehrere dedizierte Instanzen virtueller Maschinen. Jede virtuelle Maschine isoliert den Mandantenbetrieb auf der Betriebssystem-, Datenbank- und Applikationsserverebene.

Alle Software-Komponenten sind für die jeweilige Kundeninstanz reserviert und werden niemals für mehrere Kunden freigegeben.

4.3 Datenverschlüsselung

Board Cloud sichert Daten sowohl während der Übertragung als auch im Ruhezustand mit starken Verschlüsselungsalgorithmen.
Board Cloud verwendet eine Festplattenverschlüsselung, um Daten im Ruhezustand zu schützen. Alle Backups von Kundeninformationen sind ebenfalls verschlüsselt.

Die gesamte Kommunikation und die Daten in Board sind verschlüsselt. Board verwendet für alle Verbindungen digitales SSL.

Die Daten im Ruhezustand werden mit einer AES 256-Bit-Kodierung verschlüsselt, einer der stärksten Blockverschlüsselungen überhaupt.

Die Daten werden während der Übertragung mit TLS 1.2 durch ein 2048-Bit-RSA-Zertifikat mit SHA256 geschützt.

5. Sicherheitsmaßnahmen in der Board Cloud

5.1 Leistungserbringung durch Board

Nach der Vertragsunterzeichnung erfolgt die Leistungserbringung der Board Cloud.
Nach der erfolgreichen Bereitstellung der Kundeninstanz in der Board Cloud durch das Cloud Operations-Team wird eine Reihe von E-Mails an den im Vertrag festgelegten autorisierten Kundenverteiler gesendet.
Der Prozess läuft wie folgt:

1. Eine initiale Begrüßungs-E-Mail wird versendet. Diese E-Mail informiert den Ansprechpartner beim Kunden darüber, dass eine weitere E-Mail mit Details zur Aktivierung des neuen Kontos im Board Cloud Administrationsportal folgt.
2. Anschließend wird eine zweite E-Mail an den Hauptkontakt des Kontos mit dem in Punkt 1 erwähnten Aktivierungslink gesendet. Nach dem Anklicken gelangt der Benutzer zu einer Seite, von der aus er ein Konto in einem Board Cloud Administrationsportal anlegen kann.
3. Nachdem das Board Cloud Administrationsportalkonto erstellt wurde (Schritt 2), wird eine dritte E-Mail verschickt, in der der Benutzer aufgefordert wird, das neue Konto zu aktivieren. Dies geschieht durch Anklicken des in der E-Mail enthaltenen Aktivierungslinks.
4. Eine abschließende E-Mail wird gesendet, die die erfolgreiche Account-Einrichtung für das Board Cloud Administrationsportal bestätigt. Der Benutzer wird dann aufgefordert, den ersten Board-Nutzer innerhalb der Board-Anwendung anzulegen.

Sobald der Kunde die oben beschriebene Aktivierung durchgeführt hat, gilt die Bereitstellung als abgeschlossen.

5.2 Single Sign-On-Authentifizierung

SSO (“Single Sign-On”) ermöglicht es Administratoren der Anwendung, den Zugriff auf die Board Cloud-Lösung durch die Integration mit Kunden-Authentifizierungsmechanismen zu ermöglichen.

Board unterstützt die Benutzerauthentifizierung über eine föderierte Identität.
Board unterstützt die Security Assertion Markup Language (SAML 2.0) vollumfassend.

5.3 Passwort

Anforderungen an die Komplexität des Passworts:

- **Mindestens 8 Zeichen**
- **Mindestens ein Großbuchstabe**
- **Eine Zahl und ein Sonderzeichen**
- **Ablauf nach 90 Tagen**
- **Historie der letzten 5 verwendeten Passwörter**

Fünf Anmeldeversuche: Wenn ein Benutzer 5 Mal ein falsches Passwort eingibt, wird der Login für 30 Minuten deaktiviert.

5.4 Protokollierung & Auditierbarkeit

Alle Zugriffe werden überwacht und protokolliert.
Die unbefugte Verarbeitung von Informationen wird durch den Einsatz einer speziellen Software verfolgt, die Cloud-Umgebungen überwacht, um deren Verfügbarkeit und Leistung aufrechtzuerhalten.

Darüber hinaus werden moderne Intrusion Detection Systeme in der gesamten Cloud-Umgebung konfiguriert.
Zugriffe aller Systemadministratoren werden protokolliert und die Protokolldateien werden sicher auf einem Azure-Repository gespeichert.

Auch jeder Zugriff des Board Cloud Operation Teams auf die Cloud-Umgebung wird protokolliert.
Alle Benutzerzugriffe werden ebenfalls protokolliert und dem Kunden über das Board Cloud Administrationsportal zur Verfügung gestellt.

Der Kunde hat außerdem die Möglichkeit, seine Protokolle zu verschlüsseln.

5.5 Zugang und Kontrolle der Board-Mitarbeiter

- **Ausschließlich das Cloud Operation Team kann auf die Board Cloud Ressourcen zugreifen. Dieser Zugriff ist nur mit Two Factor Authentication (2FA) möglich. Der Zugriff auf jeden Rechenzentrumsserver ist zusätzlich durch ein SSL-VPN geschützt, das ein Zertifikat mit persönlicher Verschlüsselung verwendet.**
- **Board-Mitarbeiter und das Cloud Operation Team haben keinen Zugriff auf Kundendaten.**

6. Betriebliches Kontinuitätsmanagement

Board verfügt über ein klar definiertes Governance-System für Informationssicherheit. Dieses System wurde in Übereinstimmung mit den Regeln und Kriterien der Best Practices der Industrie und der internationalen Referenznormen (ISO) definiert.
Das von Board entwickelte Information Security Management System beinhaltet auch Aspekte des Betrieblichen Kontinuitätsmanagement (wie von ISO - A17. - Informationssicherheitsaspekte des Business Continuity Managements gefordert), um die Verfügbarkeit und Integrität des Services und aller darin gespeicherten Daten zu gewährleisten. Um diese Anforderungen einzuhalten, hat das Unternehmen die im Folgenden beschriebenen Maßnahmen, Best Practices und Verfahren implementiert:

- **Datenereignis: Verfahren zur Gewährleistung der Kontinuität und Vermeidung von Datenverlust durch die Backup-/Wiederherstellungsstrategien;**
- **Systemereignis: Maßnahmen und Verfahren zur Gewährleistung der Kontinuität des Services und der Wiederherstellung im Fehlerfall;**
- **Überwachungsrichtlinien und -verfahren, um bei einem Ausfall kritischer Services oder bei kritischen Datenproblemen sofort handeln zu können. Das Überwachungssystem kontrolliert den Systemzustand, indem es sowohl Daten als auch Systemereignisse wie Netzwerkkapazität, Hardware-Performance/ Ausfall und Cyber-Angriffe analysiert.**

Ebenfalls implementiert sind spezielle Richtlinien und Maßnahmen für die Verwaltung der Redundanz und der Datenverfügbarkeit innerhalb der Cloud-Umgebung. Dies wird im Folgenden erläutert:

Redundanz und Verfügbarkeit der Rechenzentren
Board Cloud wird exklusiv auf Microsoft Azure in seinen weltweit verteilten Rechenzentren eingesetzt.
Alle Rechenzentren sind als ANSI/TIA-942 Tier 4 klassifiziert, der höchsten Stufe für das Hosting unternehmenskritischer Computersysteme. Sie werden mit vollständig redundanten Subsystemen für maximale Sicherheit betrieben.
Der Einsatz von Azure-Rechenzentren ermöglicht:

- Isolierung von Daten innerhalb einer gewünschten Region, um die lokalen Richtlinien und regulatorischen Anforderungen in Bezug auf die Verarbeitung und Speicherung personenbezogener Daten oder Finanzdaten zu erfüllen.
- Auswahl eines Rechenzentrums in der Nähe der Nutzerbasis des Kunden.

Board Redundanz- und Verfügbarkeits-Services
Jeder Kunde verfügt über eine dedizierte Umgebung, die aus einem Pool von Ressourcen wie virtuellen Maschinen und Speicherbereichen besteht.
Die Redundanz und Verfügbarkeit des Ressourcenpools werden durch eine mehrschichtige, redundante Architektur gewährleistet. Sie wird über zwei Rechenzentren und Überwachungswerkzeuge repliziert, die die Überprüfung der Servicekontinuität durchführen.

Board Datenredundanz und Verfügbarkeit
Alle Kundendatenspeicher werden synchron im selben Rechenzentrum (in dem sich die Live-Daten befinden) und asynchron in einem sekundären Rechenzentrum innerhalb der zugehörigen Azure-Affinitätsregion repliziert.

Alle mit Disaster Recovery verbundenen Daten (Kundendaten, Konfigurationsdaten, Umgebungseinstellungen, die für die Wiederherstellung des Full Service notwendig sind) sind über 3 Ebenen organisiert:

1. Rechenzentrumsebene

Alle Daten (Virtual Machine Image, Shared Storage, Umgebungskonfiguration und Einstellungen) werden auf einem dedizierten Speicher vorgehalten. Sie sind lokal redundant und georedundant.

2. Instanzebene

Für jede Instanz der Board Virtual Machine wird einmal täglich ein Voll-Backup gemäß den folgenden Speicherungsrichtlinien durchgeführt:

- letzte 15 Tage rollierend: Abbild der gesamten virtuellen Maschine;
- letzte 3 Monate rollierend: Abbild der gesamten virtuellen Maschine, aufgenommen am ersten Tag des Monats.

3. Kundendatenebene

Vollständiges Backup der Kundendaten, das täglich mit den folgenden Speicherungsrichtlinien durchgeführt wird:

- letzte 15 Tage rollierend: Abbild der Datendateien des Dateisystems (alle Daten, die unter dem Pfad C:\Board gespeichert sind);
- letzte 3 Monate rollierend: Abbild des Board-Pfades am ersten Tag des Monats.

Der Kunde muss außerdem eine Komplettsicherung seiner Daten mit der **Self-Service-Backup-Funktion** durchführen und einen eigenen Backup-Plan erstellen.

7. Vorfallmanagement zur Informationssicherheit

Das Unternehmen wendet ein spezielles Verfahren an zum Tracken, Verwalten und Überwachen aller sicherheitsrelevanten Vorfälle oder Ereignisse.
Vorrangiges Ziel ist es, die bestmögliche Informationssicherheit sowie ein Höchstmaß an Servicequalität und Verfügbarkeit zu gewährleisten.

Dies wird durch die folgenden Punkte erreicht:

- **Definition einer angemessenen Managementstruktur, um auf unerwünschte Ereignisse vorbereitet zu sein, angemessen reagieren zu können und den Schaden möglichst gering zu halten;**
- **Ernennung von geeignetem Personal, die bei Vorfällen mit der erforderlichen Verantwortung, Autorität und Kompetenz reagieren und die Aufrechterhaltung der Informationssicherheit gewährleisten;**
- **Entwicklung und Genehmigung von dokumentierten Plänen, Reaktions- und Wiederherstellungsverfahren, die detailliert beschreiben, wie das Unternehmen mit einem unerwünschten Ereignis umgehen muss und wie die Informationssicherheit auf einem vorgegebenen Niveau aufrechterhalten wird, basierend auf vereinbarten Zielen der Informationskontinuität.**

Ereignisse im Bereich der Informationssicherheit müssen unverzüglich dem Information Security Manager mitgeteilt werden.

Im Falle einer Verletzung der Sicherheitsdaten wird der Kunde benachrichtigt. Zur Behebung des Problems wird rechtzeitig ein gemeinsamer Maßnahmenplan umgesetzt.

8. Lebenszyklus der Board Software-Entwicklung

Board legt besonderen Wert auf die Sicherheit während sämtlicher Stadien der Software-Entwicklung.
Board entwickelt seine Software nach agilen Methoden, die aus bestimmten Phasen besteht:

1. Analyse & Design

Die Entwicklung des Board-Produkts und seiner Eigenschaften beginnt mit der Erfassung und Analyse der Anforderungen. Das Entwicklungsteam analysiert jedes Feature und ermittelt die möglichen Risiken.
Es werden Gegenmaßnahmen ergriffen, um mögliche Risiken zu verhindern und abzuschwächen.

2. Entwicklung

Um alle Releases sicher und geschützt durchzuführen, folgt das Entwicklungsteam einer Checkliste für IT-Sicherheitsmaßnahmen.
Das System ist gegen die Top 10 der OWASP ‘Open Web Application Security Project’ Risiken geschützt.

3. Test

Für Sicherheitsthemen werden spezielle Testfälle erstellt und während des Entwicklungsprozesses ausgeführt. Das Testen umfasst Systemebene, Funktionsebene und Penetrationsebene. Testfälle betrachten die End-to-End-Version eines neuen Produkts, um Sicherheitsprobleme innerhalb des neuen Produkts zu identifizieren. Es werden spezielle Code-Tests durchgeführt, die die neuen Funktionen des Produkts enthalten.

4. Bereitstellung

Die Entwicklungsabteilung ist über einen Schwachstellenmanagementprozess in die Implementierung eingebunden. Um Schwachstellen innerhalb des bereitgestellten Codes zu identifizieren, bewertet das Team zusammen mit externen IT-Sicherheitsexperten und Kunden jede gemeldete Schwachstelle und ermittelt geeignete Maßnahmen. Ziel ist es, Verbesserungspotenziale zu identifizieren, die das Modell zu einer sich weiterentwickelnden Einheit machen, die regelmäßig aktualisiert wird.

Alle Entwickler und Tester durchlaufen ein Sicherheitstraining, um die entsprechenden Methoden zu verbessern und zu implementieren. Diese ermöglichen es, Sicherheitstechniken anzuwenden, die die Anzahl und Schwere von Bedrohungen minimieren.
Das Entwicklungsteam von Board folgt detaillierten Standards und Techniken, um das Sicherheitssystem effektiv zu betreiben.
Board verfügt über einen Prozess der Schwachstellenbewertung/Penetrationstests, der von externen Mitarbeitern unabhängig durchgeführt wird, die sich auf Cybersicherheit spezialisiert haben. Diese Prüfung wird mindestens einmal im Jahr oder bei größeren Releases durchgeführt.

8.1 Reaktion auf Sicherheitsschwachstellen

Nach Feststellung einer Sicherheitsschwachstelle kann Board wirtschaftlich angemessene Anstrengungen unternehmen, um die Schwachstelle gemäß den folgenden Richtlinien zu beheben:

PRIORITÄT*	ZEITVORGABE	VERSION (EN)
Hoch	30 Tage	Aktive Version (d.h. zuletzt ausgeliefert) und alle unterstützten Versionen
Mittel	180 Tage	Aktive Version (d.h. zuletzt ausgeliefert)
Niedrig	Nächstes größeres Release oder schnellst möglich)	Aktive Version (d.h. zuletzt ausgeliefert)

** Die Priorität wird auf der Grundlage der aktuellen Version des Common Vulnerability Scoring System (CVSS) festgelegt, einem offenen Industriestandard zur Bewertung der Schwere von Sicherheitsschwachstellen im Computersystem. Weitere Informationen zu diesem Bewertungssystem finden Sie unter https://en.wikipedia.org/wiki/CVSS*

9. Board-Mitarbeiter

Board adressiert Sicherheit bereits in der ersten Rekrutierungsphase. Die sicherheitsrelevanten Verantwortlichkeiten sind in den Arbeitsverträgen der Mitarbeiter festgelegt und die Einhaltung wird während des gesamten Arbeitsverhältnisses überwacht. Alle Mitarbeiter, die der F&E-Abteilung zugeordnet sind, sind zur Verschwiegenheit (Geheimhaltungsverpflichtung (NDA)) verpflichtet.

Es wird sorgfältig darauf geachtet, die Referenzen und das entsprechende Maß an Hintergrundprüfungen zu bestätigen. Für Board ist es von entscheidender Bedeutung, das Fachwissen zu erhöhen und das Bewusstsein dafür zu schärfen, dass Gesetze, Richtlinien und Verfahren zur Datensicherheit vollständig eingehalten werden.

Board hat verschiedene Initiativen zur Datensicherheit ergriffen, um sicherzustellen, dass alle Mitarbeiter für ihre Aufgaben und Verantwortlichkeiten qualifiziert sind und ein genaues Verständnis dafür haben.

Das Onboarding-Training enthält einen speziellen Abschnitt, der die Sicherheit des Unternehmens behandelt. Alle von der Zentrale entwickelten Schulungsinhalte sind auf Informationssicherheit ausgerichtet.

Board führt das Programm zur Sensibilisierung für Informationssicherheit in Übereinstimmung mit den Richtlinien des Unternehmens zur Informationssicherheit durch und deckt allgemeine Aspekte ab, wie z.B.:

- **Einhalten der geltenden Regeln für die Informationssicherheit, wie sie in Richtlinien, Vorschriften, Verordnungen, Verträgen und Vereinbarungen definiert sind;**
- **Persönliche Verantwortung für eigene Handlungen und Unterlassungen sowie allgemeine Verantwortung für die Sicherung oder den Schutz von Informationen, die dem Unternehmen und externen Partnern gehören;**
- **Kenntnis grundlegender Informationssicherheitsverfahren und Basismaßnahmen (wie Passwortsicherheit, Malware-Kontrollen, Clear Desks und Clear Screen);**

10. Einhaltung gesetzlicher Vorschriften & Zertifizierungen

Board Cloud ist so konzipiert und zertifiziert, dass es die Compliance-Anforderungen erfüllt.
Um seiner Verpflichtung für die Aufrechterhaltung eines erstklassigen Sicherheitssystems nachzukommen, validiert Board u.a. die Wirksamkeit seiner Cloud-Sicherheitsmaßnahmen, indem es seine Umgebung nach international anerkannten Auditierungsstandards - SSAE 18 SOC 1 Typ II und ISAE 3402 - auditiert.
Board ist außerdem nach ISO/IEC 27001:2013 zertifiziert.

10.1 SOC 1 Type II

Der SOC (Service Organization Controls)-Report entspricht SSAE 18 (Statement on Standards for Attestation Engagements No.18) und ISAE 3402 (International Standard on Assurance Engagement No.3402) Auditing-Standards und bietet Leitlinien für Auditoren, die interne Maßnahmen in einem Dienstleistungsunternehmen wie z.B. Board bewerten, die für das interne Kontrollsystem des Kunden für die Finanzberichterstattung relevant sind.

Der SOC 1 Typ II Report bestätigt die Eignung des Designs und der operativen Wirksamkeit der IT-Kontrollen von Board Cloud, um die in der Beschreibung enthaltenen Kontrollziele über einen bestimmten Zeitraum zu erreichen.
Das SOC1-Audit wird jährlich von einem unabhängigen externen Auditor durchgeführt. Der Bericht ist auf Anfrage erhältlich.

10.2 ISO/IEC 27001:2013

Board ist stolz darauf, die ISO/IEC 27001 Zertifizierung für **Board Cloud** erhalten zu haben.
ISO/IEC 27001:2013 wurde gemeinsam von der International Standard Organization (ISO) und der International Electrotechnical Commission (IEC) veröffentlicht und ist ein weltweit anerkannter Informationssicherheitsstandard, der den Unternehmen Anforderungen an ein Information Security Management System (ISMS) stellt. Das Standard-Sicherheitsmodell basiert auf drei Säulen: Vertraulichkeit, Integrität und Verfügbarkeit von Informationsbeständen. Jeder dieser Aspekte deckt einen anderen Aspekt der Sicherheit und des Schutzes von Informationen ab.

Ein jährliches Audit wird durchgeführt, um die Einhaltung der Norm zu bestätigen. Alle drei Jahre findet eine vollständige Zertifizierung statt. Das Board ISO/IEC 27001:2013 Zertifikat kann bei Interesse eingesehen werden.
Zertifizierungsumfang ist **“das Design und die Entwicklung der Board-Plattform für Business Intelligence, Performance Management und Analytik sowie die eigene Installation, Wartung und Unterstützung durch Cloud SaaS Service (Software as a Service)”.**

Insgesamt hat Board seine Fähigkeit bewiesen, alle Prozesse im Zusammenhang mit der Board Cloud sicher zu verwalten, z.B. den Lifecycle-Entwicklungsprozess, die Bereitstellung des Board Cloud Services, die Einhaltung gesetzlicher und regulatorischer Vorschriften sowie eine kontinuierliche Überwachung der Informationssicherheit.
Darüber hinaus hat Board ein unternehmensweites Information Security Management System (ISMS) entwickelt, das auf dem ISO 27001 Framework basiert. Es enthält Richtlinien, Verfahren, Arbeitsanweisungen und Checklisten für den internen Gebrauch und wird an alle Mitarbeiter verteilt.

Der Information Security Manager (ISM) überprüft und aktualisiert regelmäßig die Sicherheitsrichtlinien. Diese Überprüfung bewertet die Verfügbarkeit, Vertraulichkeit und Integrität der Daten sowie die Konformität mit der Richtlinie zur Informationssicherheit.

11. Governance und Risikomanagement

Board führt eine jährliche Risikobewertung durch, die sich mit den Sicherheitsrisiken befasst. Im Rahmen dieses Prozesses werden Bedrohungen für die Sicherheit identifiziert und das Risiko aus diesen Bedrohungen bewertet.
Die Phase der Risikobewertung beginnt mit der Identifizierung von Risiken, der Festlegung eines Risikoniveaus durch Ermittlung der Eintrittswahrscheinlichkeit und der Auswirkungen und endet mit der Ermittlung von Kontrollen und Schutzmaßnahmen, die die Auswirkungen des Risikos auf ein akzeptables Maß reduzieren. Entsprechende Maßnahmen, Empfehlungen und Kontrollen werden umgesetzt, um die Risiken so weit wie möglich zu minimieren.
Als Teil des gesamten ISMS - Information Security Management System - Framework werden die grundlegenden Sicherheitsanforderungen ständig überprüft, verbessert und implementiert.

Dazu gehört die Überwachung der laufenden Wirksamkeit und Verbesserung des ISMS-Kontrollumfelds durch Überprüfung von Sicherheitsfragen, Auditergebnissen und Überwachungsstatus sowie durch Planung und Verfolgung notwendiger Korrekturmaßnahmen.
Jede Version der Richtlinie zur Informationssicherheit und alle nachfolgenden Aktualisierungen werden an alle relevanten Interessengruppen verteilt. Die Richtlinie zur Informationssicherheit wird allen neuen und bestehenden Mitarbeitern zur Durchsicht vorgelegt. Falls eine wesentliche Änderung der Sicherheitsanforderungen erforderlich ist, kann diese außerhalb des regulären Zeitplans überprüft und aktualisiert werden

12. Über Board

Board ist die intelligente Planungsplattform, die über 2.000 führenden Unternehmen weltweit eine effizientere Planung, verwertbare Erkenntnisse und bessere Ergebnisse bietet. Board ermöglicht es führenden Unternehmen, wichtige Erkenntnisse zu gewinnen, die Geschäftsentscheidungen vorantreiben. Die Bereiche Strategie, Finanzen und Operations werden vereint, um intelligenter zu planen und volle Kontrolle über die Performance der gesamten Organisation zu erlangen. Unternehmen können mit Board ihren gesamten Planungsprozess von der Zielsetzung bis hin zur operativen Ausführung in einer einheitlichen, benutzerfreundlichen Umgebung steuern.

Dank der Zusammenarbeit mit Board haben weltweit agierende Konzerne wie H&M, BASF, Burberry, Toyota, Coca-Cola, KPMG und HSBC eine End-to-End-Planungsplattform eingeführt – in einem Bruchteil der Zeit und Kosten, die mit herkömmlichen Lösungen verbunden wären. Board International wurde 1994 gegründet, hat 25 Niederlassungen rund um den Globus und ein weltweites Partnernetzwerk. Board wurde bereits in über 100 Ländern implementiert.

Schon lange wird Board von führenden Analysten und hochkarätigen Experten wie Gartner, BARC, Nucleus und Dresner ausgezeichnet.

DE2208U

www.board.com