SWARCO

Cloud Solutions

Security Programm Übersicht V2.0

The Better Way. Every Day.

Vorwort

SWARCO ist dem Schutz und der Sicherheit von Kundendaten verpflichtet. Durch die Bereitstellung einer End-to-End Security werden die Daten in einer skalierbaren und hochverfügbaren Umgebung gesichert. Wir bei SWARCO wissen, dass nur sichere Systeme Vertrauen schaffen können.

Transparente Security Policies ermöglichen ein Verständnis darüber, wie Daten gesichert werden. So kann SWARCO seinen Kunden ein starkes Sicherheitsgefühl vermitteln. Dank strenger operativer Kontrollen wissen die Kunden ihre Daten bei SWARCO jederzeit in guten Händen. Verarbeitung und Monitoring sensibler Daten unterliegen laufenden Qualitätskontrollen mit umfassenden Sicherheitschecks. Zusätzlich schützt ein vielschichtiges System aus Detailkontrollen Unternehmen vor rechtlicher Haftung infolge unsachgemäßen Gebrauchs bzw. Zugriffs.

In diesem Dokument werden die Sicherheitsprozesse dargestellt, die SWARCO Cloud Services für den Betrieb von Kundenumgebungen umsetzt. Zur Erreichung der Sicherheitsziele wird ein Informationssicherheitsmanagementsystem (ISMS) betrieben, welches ISO/IEC 27001 zertifiziert ist.

Inhaltsverzeichnis

1 Einführung 4
1.1 Gefahrenklassifizierung 4
1.2 Minimierung von Gefahren 4
1.3 Kontinuierlicher Verbesserungsprozess 4

2 Security Grundsätze 5
2.1 Überblick 5
2.2 Richtlinien-Updates 5
2.3 Zuständigkeiten und Verantwortlichkeiten 5

3 Betriebssicherheit 6
3.1 Change Management 6
3.2 Configuration Management / Systembasis 6
3.3 Access Management 6
3.4 Training und Sicherheitsbewusstsein 6
3.5 Incident Management 6
3.6 Endpoint Management 7

4 Physische Sicherheit 7
4.1 Facilities 7
4.2 Physischer Zugang 7
4.3 Einbruchmeldeanlage 7
4.4 Environmental Controls 7
4.5 Netzwerkkommunikation 8

5 Logische Sicherheit 8
5.1 Systemauthentifizierung 8
5.2 Netzwerkkontrolle 8

1 Einführung

1.1 Gefahrenklassifizierung

Durch die Sicherheitsrichtlinien von SWARCO sollen die folgenden Gefahren minimiert werden:

- O1: Architektur- und Rechenzentrumsschwachstellen
- O2: Ausfall der Service Plattform
- O3: Verletzung des Datenschutzes und Datenverlust
- O4: Leistungsausfall/-verminderung (Software und Hardware)
- O5: Change-Prozess-Risiken und menschliches Versagen
- O6: Kontrollverfahren für die Implementierung von Sicherheitsmaßnahmen

1.2 Minimierung von Gefahren

Dieses Dokument beschreibt die durch SWARCO Cloud Services angewendeten Gegenmaßnahmen zur Minimierung der o.g. globalen Risiken.

Risiko	Maßnahmen
Architektur- und Rechenzentrumsschwachstellen	Facilities Management
Ausfall der Service Plattform	Disaster Recovery Change management Incident Response
Verletzung des Datenschutzes und Datenverlust	Data Backup Incident Response Authentication management
Leistungsausfall/-verminderung (Software und Hardware)	Incident Response Capacity Management
Betriebssicherheit - Change-Prozess-Risiken und menschliches Versagen	Change Management
Anlagenmanagement	CMDB Management Change Management Deployment of Products & Services

1.3 Kontinuierlicher Verbesserungsprozess

Als Teil der Integration der ITIL Richtlinien in die Change Management Prozesse implementiert SWARCO einen kontinuierlichen Verbesserungsprozess der zur globalen Sicherheitsstruktur gehörenden Komponenten. Aus diesem Grund behält sich SWARCO das Recht vor, ggfls. Inhalt und Qualität der beschriebenen Elemente aus dem vorliegenden Dokument anzupassen.

2 Security Grundsätze

2.1 Überblick

Das durch SWARCO Cloud Services eingerichtete Cloud Information Security Programm umfasst zahlreiche Richtlinien zur Steuerung von Technologie, Menschen und Prozessen innerhalb der Organisation. Die obersten Führungsebenen stellen Grundwerte und Kompetenzen der Organisationen auf. SWARCO Cloud Service hat ein ISMS aufgebaut, das sich an den internationalen Standards der Normenreihe ISO/IEC 27001 ff. orientiert und nutzt auf ITIL basierende Prozesse für Incident- und Change-Management-Vorgänge in seiner betrieblichen Tätigkeit. Auf diese Weise optimiert SWARCO Planung, Durchführung und Monitoring des Betriebs.

Richtlinie	Zweck
Authentication Management	Authentication Management gewährleistet eine sichere Authentifizierung beim Zugriff auf SWARCO Cloud Services-Systeme und zugehöriger Infrastruktur.
Incident Management	Incident Management legt fest, wie SWARCO bei Security Incidents und/oder gemeldeten Sicherheitslücken zu reagieren hat. Dies umfasst interne und ggfls. externe Nachforschungen, Schadensbegrenzung, Meldepflicht (soweit anwendbar), Änderungen bei der Sicherheitskontrolle und Dokumentation.
Change Management	Der Zweck dieser Richtlinie ist es, den sicheren Betrieb von SWARCO`s Infrastruktur (IS) auch bei notwendigen Changes zu gewährleisten. Um wertsteigernd zu sein sowie möglichen Beeinträchtigungen entgegen zu wirken, erfordern Changes eine gute Planung, Monitoring, Tests und Validierung.
Data Backup	Dient SWARCO Cloud Services zur Orientierung bei der Aufstellung der Datensicherungs- und -wieder-herstellungs-Pläne für Kunden, die SWARCO Cloud Services in Anspruch nehmen. Backup-Lösungen sind ein zentrales Element des flexiblen, skalierbaren, und ständig verfügbaren Sicherheitssystems der SWARCO Cloud Services.

2.2 Richtlinien-Updates

Zusätzlich zu den Cloud Policies richtet sich SWARCO nach umfangreichen internen Richtlinien und Prozessen, zu denen jeweils begleitende Dokumentation vorliegt. Die internen durch SWARCO aufgestellten Anforderungen sehen die Überarbeitung der Richtlinien mindestens einmal pro Jahr bzw. bei wichtigen Veränderungen vor.

2.3 Zuständigkeiten und Verantwortlichkeiten

Sicherheitsgrundsätze wie Aufgabentrennung und Prinzip der geringsten Rechte sind Bestandteil jeder Richtlinie und jedes Prozesses. Der durch SWARCO befolgte Change Management-Prozess basiert auf den ITIL-Richtlinien, trennt Einheiten mit Sicherheitsaufgaben von allgemeinen Verwaltungsaufgaben, führt eine Dokumentation und/oder Genehmigung für Changes oder Zugangsanfragen und wird getragen von der Lösungskompetenz einer IT Service Management-Lösung.

Sicherheitszuständigkeiten und -verantwortlichkeiten werden getrennt von allgemeinen System- und Netzwerkadministrationsfunktionen verwaltet. Auditierende Funktionen werden durch die ISMS-Organisation innerhalb von SWARCO bzw. durch externe Audits (z.B. für ISO/IEC 27001-Zertifizierungen) wahrgenommen. Risiko- und Vulnerability Management werden durch die o.g. ISMS-Organisation überwacht.

3 Betriebssicherheit

3.1 Change Management

Systeme unterliegen bei SWARCO einem ausführlichen Prozess für Changes, eingeschlossen Patch- und Konfigurationsverwaltung. Change Requests werden in einem standardisierten Verfahren bearbeitet. So ist sichergestellt, dass alle Changes freigegeben und registriert sind. Ereignisse, die eine hohe Auswirkung haben könnten, werden durch ein Change and Review Board (CRB) sowie durch ein Change Advisory Board (CAB) besprochen und bewertet, um Beeinträchtigungen von Vertraulichkeit, Integrität oder Verfügbarkeit eines Systems durch einen umgesetzten Change auszuschließen. Der durch SWARCO eingesetzte Change Management-Prozess basiert auf den ITIL-Best Practises.

3.2 Configuration Management / Systembasis

Innerhalb der zentralisierten Lösung, die im Rahmen der Cloud Services Anwendung findet, unterhält SWARCO exakte und relevante Systemgrundlinien für Hardware und Software, die jährlich einem Review unterzogen werden. Eine umfassende Systemliste erlaubt SWARCO Cloud Services eine wirkungsvolle Verwaltung von Anpassungen an Kundenumgebungen. Es erfolgen Anpassungen im Rahmen des Changemanagement-Prozesses.

3.3 Access Management

Über die eingebauten Fähigkeiten einer ITSM Solution sorgt SWARCO Cloud Service für den ungehinderten Datenfluss unter Berücksichtigung der erforderlichen Genehmigungen durch die Vorgesetzten der Anforderer, das entsprechende Führungsteam sowie durch die SWARCO Security Organisation. Der Zugang wird jährlich überprüft und wird geändert bei jeder Änderung des Personals.

3.4 Training und Sicherheitsbewusstsein

Alle SWARCO-Mitarbeiter sowie durch SWARCO beauftragte Auftragnehmer/Lieferanten mit Zugang zu den Kundensystemen müssen ein Sicherheitstraining und eine Schulung zum Sicherheitsbewusstsein absolvieren, bevor ein Zugang ermöglicht wird. Hierbei ist eine jährliche Auffrischung erforderlich. Erfolgt dies nicht, wird der Zugang gesperrt. Der Zugang wird initial festgelegt während des Einstellungsprozesses vor Zuteilung. Bei der Definition einer bestimmten Stelle innerhalb der Organisation legen der einstellende Manager sowie HR die Anforderungen hinsichtlich Zugangslevel, Security-Verantwortlichkeiten und Kontrolle fest, die für die jeweilige Position notwendig sind. Der Security-Beauftragte prüft den Zugang jährlich.

3.5 Incident Management

Um schnell auf Sicherheits- oder Datenschutz-Incidents reagieren zu können, hat SWARCO Cloud Services ein Privacy and Security Incident Response Team (PSIRT) gebildet. Das PSIRT bearbeitet alle Meldungen bzgl. Datenschutz- und Sicherheits-Incidents bzw. bzgl. Sicherheitslücken. Alle Informationen zu einem entsprechenden Incident werden gesammelt und nach den eingesetzten Verfahren vollständig dokumentiert.

3.6 Endpoint Management

Alle SWARCO-Mitarbeiter sowie durch SWARCO beauftragte Auftragnehmer/Lieferanten mit Zugang zu sensiblen Kundendaten unterliegen der strikten Einhaltung der Sicherheitsrichtlinien bzgl. der durch die SWARCO IT definierten und durchgesetzten Regeln zur Arbeitsplatzrechner-Sicherheit.

4 Physische Sicherheit

Während der Begutachtung der Private und/oder Public Cloud-Umgebungen stellt SWARCO sicher, dass sich die/der IaaS Provider bzgl. der physischen Zutrittskontrolle und -verfolgung nach den einschlägigen Sicherheitsregeln richten. SWARCO kann diese Regelungen durch VorOrt-Kontrollen, Audits von dritten Parteien sowie durch Zertifizierungen wie ISO27001, ISO9001 und SSAE16/SOC1 bestätigen lassen.
Obwohl diese Sicherheitsregeln je nach Provider variieren können, repräsentieren die im Folgenden aufgeführten Mindestspezifikationen die Anforderungen, die SWARCO Cloud Services von den Providern verlangt.

4.1 Facilities

Rechenzentren, die sensitive Kundendaten speichern, empfangen oder übertragen, werden strategisch ausgesucht, um hochriskante Ereignisse wie Naturkatastrophen, eingeschlossen Risiken der höheren Gewalt, zu verhindern.

4.2 Physischer Zugang

SWARCO ist zur Implementierung von Prozessen und Richtlinien verpflichtet, um alle Anlagen und Einrichtungen gegen physischen Zugriff, Sabotage oder Diebstahl zu schützen. In den SWARCO Richtlinien ist ein begrenzter und kontrollierter Zugang zu Anlagen mit Informationssystemen geregelt. Dies schließt die Zugangskontrolle von Mitarbeitern entsprechend ihrer Funktion ein. Ebenso eingeschlossen ist die Besucherkontrolle.

4.3 Einbruchmeldeanlage

Mit den implementierten Systemen, die jeden Zutritt überwachen, wird der Zugang zu Räumlichkeiten, in denen sich sensitive Kundendaten befinden, nur für autorisiertes Personal erlaubt. Wenn möglich, wird der Zugang durch eine multi-factor Zugangskontrolle autorisiert. Die Rechenzentren sind darüber hinaus durch zusätzliche Sicherungssysteme geschützt, um unautorisierte Zutritte zu verhindern, wie z.B.:

- Überwachungskameras, CCTV (Closed-Circuit Television)
- …

4.4 Environmental Controls

Wo Rechentechnik und Speichergeräte untergebracht sind, werden ständig Messungen vorgenommen, um optimale Bedingungen für Rechner z.B. hinsichtlich Temperatur und Luftfeuchtigkeit zu gewährleisten. Um die Risiken von ungünstigen klimatischen Bedingungen zu minimieren, werden kritische Systeme redundant eingesetzt. Die folgenden Steuerungen sind implementiert zum Schutz vor Feuer bzw. Überflutung, Stromausfall und anderen Umgebungsbedingungen, die zu einem Ausfall der Services führen können:

- Zentrale Alarmierung mit direkter Kommunikation zu Notdiensten
- Feuermeldesysteme
- Feuerbekämpfungssysteme
- USVs
- Redundante Auslegung kritischer Systemkomponenten für den Failover-Fall

Obwohl ein „defense-in-depth“-Konzept keine Garantie ist, dass ein Ausfall ausgeschlossen ist, werden die folgenden Regelungen sicherstellen, dass die Verfügbarkeit zu einem angemessenen Grade gewährleistet wird. Wenn Geschäftsbedürfnisse zusätzliche Maßnahmen bzgl. der Verfügbarkeit begründen, kann SWARCO Cloud Services die Fähigkeit der Bereitstellung von DR-Services gewährleisten.

4.5 Netzwerkkommunikation

Die Räumlichkeiten sind so ausgelegt, dass sie Beeinträchtigungen des Netzwerks, die die Integrität der Datenverarbeitung betreffen, verhindern. So können gegen solche Beeinträchtigungen resistente Technologien wie Glasfaser oder abgeschirmte Verkabelung eingesetzt werden. Das kann helfen bei der Eliminierung oder Reduktion von Beeinträchtigungen auf Grund von elektr. Rauschen, elektromagnetischen oder anderen Störungen.
Kritische Netzwerk-Komponenten sind mehrfach vorhanden und werden überwacht und geschützt durch Sicherheitslösungen wie Firewall, Host/Netzwerk basierende IDS und Anti-Malware-Lösungen. Alle Verbindungen, die für die Verwaltung der Systeme genutzt werden, sind gesichert durch private Kommunikationskanäle wie VPNs.

5 Logische Sicherheit

5.1 Systemauthentifizierung

Jeder Benutzer erhält ein eigenes Kennwort, das auf die persönliche Nutzung beschränkt ist. Dienst-Accounts sind auf Mitarbeiter beschränkt, die den Zugang aufgrund ihrer Rolle im Unternehmen benötigen. Die Accounts werden regelmäßig überprüft, um unbefugten Zugriff auszuschließen.

Im Rahmen der Verwaltung des Account-Lebenszyklus für alle Nutzer werden regelmäßige Checks durchgeführt. Auf Grundlage einer SWARCO Access Management-Richtlinie werden Account-Anträge bearbeitet, geprüft und abgeschlossen. Jeder Account-Antrag wird im Detail dokumentiert. Dabei wird der Account-Typ festgehalten und die Ressourcen, auf die Zugriff gewährt wird.

5.2 Netzwerkkontrolle

Der Zugang zu SWARCO Cloud Services Systemen ist auf Nutzer innerhalb des SWARCO-Netzwerks begrenzt. Darüber hinaus werden nur durch SWARCO freigegebene Geräte für die SWARCO Cloud zugelassen.

Zur Authentifizierung gegenüber den Informationssystemen werden ausschließlich sichere Protokolle verwendet. Außerdem laufen Remote Sessions in zuvor festgelegten Zeitabständen aus, um zu gewährleisten, dass nur autorisierte Nutzer auf die Systeme zugreifen. Remote Sessions werden verschlüsselt, um die Vertraulichkeit des Kommunikationsverkehrs zu schützen.