Technische und organisatorische Maßnahmen (TOMs)

Diese technischen und organisatorischen Maßnahmen beschreiben die Implementierung von Maßnahmen zur sicheren Verarbeitung personenbezogener Daten gemäß den anwendbaren Datenschutzgesetzen. Die Anforderungen von Artikel 24, 25 und 32 DSGVO werden, soweit anwendbar, berücksichtigt.
Die nachstehenden Spezifikationen gelten für die folgenden physischen Standorte: die Unternehmenszentrale Checkmk GmbH in München (DE) und Checkmk, Inc. in Atlanta (USA), die Standorte der Rechenzentren und die Heimarbeitsplätze (Home Offices) der Mitarbeitenden (Ausnahme: physischer Zugang).

1. Vertraulichkeit

1.1. Physischer Zugang

1.1.1. Allgemeines Konzept:
Alle Räume, in denen personenbezogene Daten verarbeitet oder Geräte aufbewahrt werden, die zur Verarbeitung personenbezogener Daten dienen, müssen der aktuellen Fassung der Richtlinie zur physischen Sicherheit entsprechen. Die wichtigsten Datenverarbeitungsressourcen befinden sich in einem externen Rechenzentrum, das nach den in Ziffer 1.1.2 genannten einschlägigen Industriestandards zertifiziert ist. Detaillierte Maßnahmen zur Implementierung des Konzepts im Unternehmen:

Die wichtigsten Ressourcen für die Speicherung und Verarbeitung von Daten befinden sich in einem externen Rechenzentrum („RZ“), das mindestens nach ISO 9001, ISO 27001, ISO 22301, ISO 27701, ISO 27017, ISO 27018, SOC 2 Type II zertifiziert oder zugelassen ist. Anwendungen, die als „Software as a Service“ angeboten werden, werden in den Rechenzentren von Amazon Web Services gehostet; siehe auch https://aws.amazon.com/compliance/data-center/controls/. Bei Unstimmigkeiten zwischen den nachstehend aufgeführten Maßnahmen und den auf der Website von Amazon Web Services aufgeführten Maßnahmen haben letztere Vorrang.

- Verschlossenes Gebäude (außer Niederlassung Atlanta)
- Verschlossene Büroräume
- Elektronisches Sicherheitsschließsystem
- Mechanisches Sicherheitsschließsystem
- Physisches Zugangskontrollsystem
- Funktionsbasierte physische Zugangskontrollen
- Biometrisches Zugangskontrollsystem (nur RZ)
- Verschlossene Server-Räume
- Verschlossene Server-Schränke
- Verschlossene Server-Räume mit Zugangskontrolle (nur RZ)
- Videoüberwachung (nur RZ)
- Alarmsystem (nur RZ)
- Dokumentierte Schlüsselausgabe
- Zentraler Empfangsbereich
- Besucherregistrierung
- Besucherüberwachung

- Besucheridentifizierung mit Besucherausweis
- Definition der Sicherheitsparameter
- 24/7 Sicherheitspersonal vor Ort (nur RZ)
- Richtlinie für physische Sicherheit

1.2. Authentifizierung

1.2.1. Allgemeines Konzept:
Für jeden Benutzer werden eindeutige Benutzerkonten erstellt, die mit einem Passwort ausreichender Länge und Komplexität geschützt werden müssen. Die Passwortregeln werden zentral durchgesetzt und Login-Versuche engmaschig überwacht. Für wichtige Anwendungen ist eine sichere Verbindung und eine 2-Faktor-Authentifizierung erforderlich. Der Zugang zu Administrator-Schnittstellen ist auf eine minimale Gruppe von IT-Administratoren begrenzt und erfordert eine Multifaktor-Authentifizierung sowie eine verschlüsselte Verbindung. Die Nutzung von Unternehmenseigentum ist durch eine Nutzungsrichtlinie geregelt.

1.2.2. Wesentliche Maßnahmen zur Implementierung des Konzepts im Unternehmen. Bitte entnehmen Sie weitere Details der aktuellen Version den jeweiligen Richtlinien, wie nachstehend aufgeführt:

- Eindeutige Benutzerkonten
- Zentral verwaltete Authentifizierung mit Benutzernamen und Passwort
- Die Passwortkonvention schreibt komplexe Passwörter mit mindestens 12 Zeichen vor.
- Automatisierte Kontrolle der Passwortkonvention
- Multifaktor-Authentifizierung für wichtige Anwendungen
- Multifaktor-Authentifizierung für Administratorschnittstellen
- Zugangssperre nach wiederholter Eingabe falscher Login-Daten
- Laufwerkverschlüsselung
- Zugang zu Datenverarbeitungsanwendungen nur über VPN-Verbindung
- Implementierung einer Endpoint Management Software oder vergleichbarer Kontrollen
- Implementierung einer Managementsoftware für mobile Geräte
- Implementierung einer aktuellen Firewall an Endgeräten
- Implementierung eines aktuellen Virenschutzes oder kompensierender Kontrollen
- Zentrales Log-Management
- Überprüfung der Benutzeridentitäten
- Regelmäßige Prüfungen der Benutzerkonten
- Richtlinie zur Zugangskontrolle
- Richtlinie zur akzeptablen Nutzung
- Passwortrichtlinie
- Kryptografierichtlinie

1.3. Datenzugangskontrolle

1.3.1. Allgemeines Konzept:
Es gibt ein funktionsbasiertes Autorisierungskonzept. Der Zugang zu personenbezogenen Daten ist auf autorisierte Personen beschränkt und auf das für die Erfüllung ihrer Aufgaben erforderliche Maß begrenzt (Prinzip der geringsten Privilegien). Der Administratorzugang ist auf eine minimale Gruppe von IT-Administratoren beschränkt. Der Zugang auf Benutzerzugriffsprotokolle unserer Software-as-a-Service-Anwendungen ist auf Audit-Personal und Sicherheitsingenieure beschränkt. Die Zuweisung, Änderung und Entziehung von Zugriffsrechten erfolgt nach einem dokumentierten Verfahren. Privilegien unterliegen regelmäßigen Überprüfungen. Um Daten vor unbefugtem Zugriff zu schützen, werden alle Daten am Speicherort und während der Übertragung verschlüsselt. Die Speicherung von personenbezogenen Daten sowie ihre Löschung oder Vernichtung erfolgt nach dokumentierten Verfahren und anerkannten Branchenstandards. In der Regel werden für personenbezogene Daten keine Wechseldatenträger benutzt.

1.3.2. Detaillierte Maßnahmen zur Implementierung des Konzepts im Unternehmen:

- Nach Möglichkeit zentrale Verwaltung des Zugangs zu Anwendungen nach Einzelbenutzern oder Benutzergruppen
- Authentifizierung mit Benutzernamen und Passwort
- Protokollierung der Benutzerzugriffe auf sensible Dienste oder Anwendungen
- Verschlüsselung von Daten am Speicherort und bei Übertragung.
- Löschung gespeicherter Daten gemäß der Richtlinie zur Aufbewahrung von Daten.
- Vernichtung physischer Dokumente gemäß der Richtlinie zur Aufbewahrung von Daten.
- Verschlossene Schränke zur Aufbewahrung physischer Dokumente
- Sichtschutz und Sichtblenden für sensible Funktionen
- Funktionsbasiertes Autorisierungskonzept für Anwendungen und Dateien nach dem Prinzip des geringsten Privilegs
- Regelmäßige Überprüfung und Anpassung von Zugangsrechten
- Beschränkung und Dokumentation von Administratorzugängen
- Dokumentierte Verfahren für die Aufbewahrung und Löschung personenbezogener Daten
- Richtlinie zur Klassifizierung von Daten
- Richtlinie zur Aufbewahrung von Daten
- Richtlinie zur akzeptablen Nutzung
- „Clean Desk and Clear Screen“-Vorschrift
- Allgemeines Verbot, Unternehmensdaten auf Wechseldatenträgern zu speichern, gemäß der Richtlinie zur akzeptablen Nutzung

Spezifische Maßnahmen für Anwendungen, die als „Software as a Service“ angeboten werden:

- Zugang zu Benutzerzugriffsprotokollen auf Audit-Personal und Sicherheitsingenieure beschränkt

1.4. Pseudonymisierung

1.4.1. Allgemeines Konzept:
Personenbezogene Daten werden nach Möglichkeit in frühen Phasen von Analysen pseudonymisiert. Dritten wird empfohlen, Daten an der Quelle zu pseudonymisieren oder zu anonymisieren, wenn die personenbezogenen Daten nicht zur Verarbeitung benötigt werden.

1.4.2. Detaillierte Maßnahmen zur Implementierung des Konzepts im Unternehmen:

- Verwendung von Hashing-Algorithmen wo anwendbar und erforderlich
- Dritten wird empfohlen, Daten an der Quelle zu pseudonymisieren
- Pseudonymisierung in einer frühen Phase der Datenverarbeitung, wo erforderlich
- Unverzügliche Pseudonymisierung auf Aufforderung

1.5. Trennungskontrolle

1.5.1. Allgemeines Konzept:
Personenbezogene Daten werden durch den Kunden mindestens mittels logischer Trennung getrennt. In unseren "Software-as-a-Service"-Anwendungen implementieren wir ein Multi-Tenancy-Konzept mit logischer Trennung der Datenspeicherung.

1.5.2. Detaillierte Maßnahmen zur Implementierung des Konzepts im Unternehmen:

- Logische Trennung von Live- und Testumgebungen
- Physische oder logische Trennung von Anwendungen
- Logische Trennung interner Netzwerke nach Geschäftsfunktionen
- Logische Trennung von Kundendaten in Anwendungen
- Logische Trennung von Tenants (nur SaaS)
- Funktionsbasierte Zugangskontrollen
- Begrenzung des direkten Zugangs zu Datenbanken

Spezifische Maßnahmen für Anwendungen, die als „Software as a Service" angeboten werden:

- Logische Trennung von Tenants
- Logische Trennung der Speicherung von Tenant-Daten

2. Integrität

2.1. Übertragungskontrolle

2.1.1. Allgemeines Konzept:
Es wurden Maßnahmen getroffen, um die Eingabe, Änderung und Löschung personenbezogener Daten der Person zuzuordnen, die sie ausführt. Die Änderung und Löschung von Datensätzen muss beschränkt sein, damit eine versehentliche Änderung oder Löschung wirksam verhindert wird.

2.1.2. Detaillierte Maßnahmen zur Implementierung des Konzepts im Unternehmen:

- TLS-Verschlüsselung aller Daten bei Übertragung
- Zugang zu Kernanwendungen nur über VPN-Verbindung
- Verbot der Verwendung privater Speichermedien für Unternehmensdaten
- Verbot der Verwendung von Kommunikations-Accounts für private Zwecke
- Verbot der Speicherung von Unternehmensdaten auf nicht verwalteten privaten Geräten
- Verschlüsselung von Daten auf Speichermedien
- Allgemeines Verbot, Unternehmensdaten auf Wechseldatenträgern zu speichern
- Anonymisierung und Pseudonymisierung, wo anwendbar

2.2. Eingabekontrolle

2.2.1. Allgemeines Konzept:
Es wurden Maßnahmen getroffen, um die Eingabe, Änderung und Löschung personenbezogener Daten der Person zuzuordnen, die sie ausführt. Die Änderung und Löschung von Datensätzen muss beschränkt sein, damit eine versehentliche Änderung oder Löschung wirksam verhindert wird.

2.2.2. Detaillierte Maßnahmen zur Implementierung des Konzepts im Unternehmen:

- Rückverfolgbarkeit von Eingaben, Änderungen und Löschungen durch personalisierte Benutzer
- Dokumentierte Verfahren für die Vergabe, Änderung und Entziehung von Benutzerberechtigungen
- Protokollierung von Änderungen personenbezogener Daten
- Funktionsbasierte Zugangskontrollen
- Trennung von Aufgaben

2.3. Auftragskontrolle

2.3.1. Allgemeines Konzept:
Im Rahmen der Auftragskontrolle werden alle Datenverarbeitungsvorgänge, die im Auftrag des Kunden durchgeführt werden, ausschließlich auf schriftliche Anweisung des Kunden ausgeführt. Alle Mitarbeitenden, die personenbezogene Daten verarbeiten, werden regelmäßig geschult. Unterauftragsverarbeiter werden nur nach entsprechender Vereinbarung mit dem Kunden beauftragt. Sie werden sorgfältig nach einem dokumentierten Lieferantenbewertungs- und -managementprozess ausgewählt.Alle Unterauftragsverarbeiter müssen einen Datenverarbeitungsvertrag gemäß Art. 28 DSGVO schließen.

2.3.2. Detaillierte Maßnahmen zur Implementierung des Konzepts im Unternehmen:

- Dokumentation der Verarbeitungstätigkeiten
- Verarbeitung personenbezogener Daten nur mit schriftlicher Einwilligung

- Es wird sichergestellt, dass die Daten nach Abschluss des Verarbeitungsauftrags gemäß den Datenschutzbestimmungen vernichtet oder zurückgegeben werden.
- Sorgfältige Beurteilung und Auswahl der Auftragsverarbeiter
- Verpflichtung aller Auftragsverarbeiter gemäß Artikel 28 DSGVO
- Schriftlicher Vertrag mit dem Verarbeiter über den Mindestdatenschutzstandard
- Ausdrückliche Regelung zur Beauftragung weiterer Unterauftragsverarbeiter
- Nach Möglichkeit Befugnis zur Durchführung von Audits bei Auftragsverarbeitern
- Risikobasierte Überwachung der Auftragsverarbeiter
- Richtlinie zum Lieferantenmanagement

3. Verfügbarkeit und Ausfallsicherheit

3.1. Allgemeines Konzept:
In allen Rechenzentren sind Maßnahmen zur effektiven Vermeidung von Ausfallzeiten aufgrund physischer Störungen implementiert (z. B. unterbrechungsfreie Stromversorgung, Rauch- und Brandmelder, Klimaanlage). Es liegen dokumentierte Pläne zur Aufrechterhaltung der Geschäftstätigkeit und Notfallpläne vor.

3.2. Detaillierte Maßnahmen zur Implementierung des Konzepts im Unternehmen:
Die wichtigsten Ressourcen für die Speicherung und Verarbeitung von Daten befinden sich in einem externen Rechenzentrum, siehe auch 1.1.2.

- Regelmäßiges, automatisiertes und dokumentiertes Patch-Management für Server
- Regelmäßiges, zentral verwaltetes und dokumentiertes Patch-Management für Endgeräte, angepasst an das Betriebssystem
- Automatisiertes Scanning von Schwachstellen mit Alarmfunktion
- Einsatz und regelmäßige Aktualisierung einer Antivirensoftware oder kompensierender Kontrollen
- Datenspeicherung auf Speichersystem
- Kapazitätsüberwachung mit Alarmfunktion
- Räumlich redundante Datenspeicherung (nur Rechenzentren)
- Redundante Netzbetreiber (nur Rechenzentren)
- Unterbrechungsfreie Stromversorgung / USV (nur Rechenzentren)
- Notstromversorgung (nur Rechenzentren)
- Redundante Klimaregelung für Server (nur Rechenzentren)
- Temperatur- und Feuchtigkeitsüberwachung in Serverräumen (nur Rechenzentren)
- Frühzeitige Rauch- und Branderkennung (nur Rechenzentren)
- Feuerlöscher in allen Serverräumen (nur Rechenzentren)
- Notfallplan und Richtlinie zur Geschäftskontinuität
- Dokumentierte Verfahren zur Reaktion auf Vorfälle und Vorfallmanagement

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

4.1. Allgemeines Konzept:

Es wurden qualifizierte Personen als Datenschutz- und Informationssicherheitsbeauftragte ernannt und mit der Pflege, Überprüfung und regelmäßigen Aktualisierung der internen Prozesse und Verfahren betraut. Es werden dokumentierte Prozesse für die Risikobewertung und -behandlung sowie für Incident Management und Berichterstattung angewandt.
Alle Mitarbeitenden sind vertraglich zur Geheimhaltung verpflichtet und müssen regelmäßig an Awareness Trainings teilnehmen.

4.2. Detaillierte Maßnahmen zur Implementierung des Konzepts im Unternehmen:

- Ernennung eines Datenschutzbeauftragten
- Ernennung eines Informationssicherheitsbeauftragten
- Vertragliche Datenschutzverpflichtung der mit der Datenverarbeitung beauftragten Personen
- Regelmäßige dokumentierte Awareness Trainings für Mitarbeitende
- Dokumentiertes Verfahren für die Einführung, Änderung und Einstellung von Datenverarbeitungstätigkeiten
- Regelmäßige Überprüfung des Stands der Technik gemäß Artikel 32 DSGVO
- Dokumentierter Prozess zur Risikobewertung und -behandlung mit regelmäßigen Risikobewertungen