

Ergebnisse anzeigen

Auskunftsperson

9

Anonym

77:22

Zeit zum
Ausfüllen

Allgemeine Angaben

Angaben von Basisinformationen zur Beschreibung des Service bzw. des Providers

1. Firma

Mercoline GmbH

2. Ansprechpartner

Alexander Kastler

3. E-Mail / Telefon

Alexander.Kastler@mercoline.de / +49 30 436 589 - 108

4. Ist Ihr Unternehmen nach IEC/ISO 27001 oder ähnliche Informationssicherheitsnormen zertifiziert?

☐ Ja, IEC/ISO 27001

☐ Ja, andere

☒ Nein

5. Bitte füllen Sie den Fragebogen zur Informationssicherheit aus: <https://forms.office.com/r/VbtSEEfRqQ>

☒ Ja

☐ Nein

6. Es existiert eine formale, schriftlich dokumentierte IT-Security Policy?

☒ Ja

☐ Nein

7. Ist ein Datenschutzbeauftragter bestellt?

☒ Ja

☐ Nein

8. Ist ein IT-Sicherheitsbeauftragter beschäftigt?

☒ Ja

☐ Nein

9. Werden die Mitarbeiter auf das Datengeheimnis gemäß §5 BDSG verpflichtet?

- ☒ Ja
- ☐ Nein

10. Sind die Mitarbeiter hinsichtlich der Datenschutzrechtlichen Vorgaben nachweislich geschult?

- ☒ Ja
- ☐ Nein

11. Gibt es ein Verzeichnisse gem. §4 BDSG?

- ☐ Ja
- ☒ Nein

12. Wer wird bei entdeckten Sicherheitsvorfällen unverzüglich informiert?

Abhängig von dem Sicherheitsvorfall der ServiceDesk, der IT-Sicherheitsbeauftragte, oder der CISO.

13. Welche Sicherheits- und Datenschutzrichtlinien existieren bei Ihnen?

S1 Leitlinie Informationssicherheit S2 Benutzerrichtlinie Richtlinie Audit und Management-Review Richtlinie Benutzermanagement Richtlinie IT-Risikomanagement Richtlinie Klassifikation Richtlinie Kryptografie Richtlinie Lieferantenmanagement Richtlinie Mobilgeräte und mobiles Arbeiten Richtlinie Notfallmanagement Richtlinie Passwortmanagement Richtlinie Personal Richtlinie Physische Sicherheit Richtlinie Projektmanagement Richtlinie Protokollierung Richtlinie Sicherer Betrieb Richtlinie Sichere Entwicklung Richtlinie Sichere Netzwerke Richtlinie Sicherheitsorganisation Richtlinie Sicherheitsvorfälle Interessierte Parteien Sicherheitskennzahlen Relevante Gesetze

Zutrittskontrolle

Darstellung des physischen Zutritts in die Räumlichkeiten des Anbieters bzw. dessen Regelung.

14. Existiert ein schriftlich dokumentiertes Zutrittsberechtigungssystem für Mitarbeiter des Unternehmens bzw. nicht zugriffsberechtigte Personen (z.B. Geschäftskunden/Besucher, Reinigungsfirpen; Wartungsfirpen, etc.)?

☒

Ja

☐

Nein

15. Gibt es Regelungen für die Vergabe und Rücknahme von Schlüsseln/Key-Cards sowie den Wechsel von PIN-Codes?

☒

Ja

☐

Nein

16. Bestehen Regelungen bei der Vergabe, dem Entzug und dem zyklischen Review der Zutrittsberechtigungen inkl. Dokumentation der vergebenen Berechtigungen?

☒

Ja

☐

Nein

17. Bestehen dokumentierte Regelungen für den Einsatz von Servicepersonal (z.B. Wartungstechniker, Reinigungskräfte,...)?

- ☐ Ja
- ☒ Nein

18. Gibt es ein Alarmsystem?

- ☐ Ja
- ☒ Nein

19. Fenster im Erdgeschoss sowie Schächte sind gesichert?

- ☒ Ja
- ☐ Nein

20. Stehen sämtliche Server-Systeme nur in besonders gesicherten Räumen?

- ☒ Ja
- ☐ Nein

21. Befinden sich die Server in abschließbaren und abgeschlossenen Serverschränken?

- ☒ Ja
- ☐ Nein

22. Es gibt Regelungen zu Vergabe, Entzug und zyklischen Review von Zugangsberechtigungen? Relevant sind die Ebenen: Anmeldung am Netzwerkgerät, z.B. Firewall

☒

Ja

☐

Nein

Verfügbarkeit

Beschreibung des Betriebs bzw. der Sicherstellung des Betriebs.

23. Existiert ein Backup- und Recoverykonzept mit täglicher/regelmäßiger Sicherung?

☒

Ja

☐

Nein

Datenschutz & Security

Darstellung der technischen und organisatorischen Maßnahmen zur Gewährleistung des Datenschutzes.

24. Existiert ein Datenschutz bzw. Sicherheitskonzept für die Anwendung?

☐

Ja

☒

Nein

25. Es gibt Regelungen zu Vergabe, Entzug und zyklischen Review von Zugangsberechtigungen? Relevant sind die Ebenen: Anmeldung an der Applikation)

☒

Ja

☐

Nein

26. Existiert die Möglichkeit inaktive Benutzer (z.B. kein Login innerhalb von 90 Tagen) zu identifizieren und zu deaktivieren?

☐

Ja

☒

Nein

27. Werden sämtliche Berechtigungen lediglich auf der Basis der minimalen Rechte (Need-To-Know) vergeben?

☒

Ja

☐

Nein

28. Ist ein Zugang nur mit Authentifizierung möglich? Relevant sind die Ebenen Netzwerk, Betriebssystem und Applikation

☒

Ja

☐

Nein

29. Existieren Maßnahmen zum Schutz von Passwortdateien und Passwörtern auf der Applikationsebene?

☒

Ja

☐

Nein

30. Existieren Maßnahmen gegen Brute-Force bzw. Denial-of-Service-Angriffe auf den Anmeldungs-Service?

- ☐ Ja
- ☒ Nein

31. Es gibt Regelungen zu Vergabe, Entzug und zyklischen Review von Zugangsberechtigungen? Relevant sind die Ebenen: Anmeldung am Service, Betriebssystem, z.B. SSH)

- ☒ Ja
- ☐ Nein

32. Ist ein Zugang nur mit Authentifizierung möglich? Relevant sind die Ebenen Netzwerk und Betriebssystem.

- ☒ Ja
- ☐ Nein

Zugang & Berechtigung

Darstellung des Zugangs und Berechtigung auf technischer Ebene bzw. dessen Regelung.

33. Es gibt Regelungen zur Vergabe, Verwaltung und zum (zeitnahen) Entzug von Zugriffsberechtigungen (Berechtigungskonzept?) Relevant sie dabei die Ebenen der Anwendung, der Datenbank, des Betriebssystems und des Netzwerks.

☒

Ja

☐

Nein

34. Existiert ein Berechtigungskonzept für die Applikation zur bedarfsorientierten Ausgestaltung der Zugriffsrechte (differenzierte Berechtigungen für Profile, Rollen, Transaktionen und Objekte)?

☒

Ja

☐

Nein

35. Zugriffsberechtigungen sind abhängig von der jeweiligen Funktion?

☒

Ja

☐

Nein

36. Wie und wo erfolgt die Trennung der Daten von Daten anderer Kunden?

Logische Trennung auf Basis der Clients.

37. Erfolgt die Speicherung von sensitiven Daten verschlüsselt?

☒

Ja

☐

Nein

38. Wo sind die Schlüssel für die Datenverschlüsselung hinterlegt? Wer hat die Hoheit über die Schlüssel?

Lokal auf dem Server. Die Hoheit liegt bei dem Administrator.

Service & Support

Darstellung der für die Bereitstellung des Services und Gewährleistung der SLA notwendigen Prozesse.

39. Existiert ein Notfallkonzept/-Handbuch?

- ☐ Ja
- ☒ Nein

40. Existiert ein Betriebshandbuch?

- ☐ Ja
- ☒ Nein

Portabilität

Darstellung der technischen und fachlichen Voraussetzungen zur Migration und Wechsel des Services.

41. Wie sieht die Ausstiegsstrategie (Exit) aus? Können die Daten über Standardschnittstellen exportiert und in andere Systeme übernommen werden?

Nein