

Ergebnisse anzeigen

Auskunftsperson
6 Anonym

18:38
Zeit zum
Ausfüllen

1. Unternehmen *

Mercoline GmbH

2. Ansprechpartner *

Alexander Kastler

3. Besteht bereits eine Zertifizierung nach ISO 27001? *

- ☐ Ja
- ☒ Nein

4. Existiert im Unternehmen einen namentlich benannter Informationssicherheitsbeauftragter?

- ☒ Ja
- ☐ Nein

5. Name des Informationssicherheitsbeauftragten

Alexander Kastler

6. Besteht ein Information Security Management System (ISMS)?

- ☒ Ja
- ☐ Nein

7. Gibt es im Unternehmen eine Informationssicherheitsleitlinie?

- ☒ Ja
- ☐ Nein

8. Wie ist die Informationssicherheit im Unternehmen organisiert?

Zur Sicherstellung der Informationssicherheit - Vertraulichkeit, Verfügbarkeit und Integrität sämtlicher Daten und Informationen - für DATAGROUP und deren Kunden - wurde das DATAGROUP ISMS (Information Security Management System) gemäß ISO/IEC 27001 implementiert.

Im Rahmen des DATAGROUP ISMS werden eine Sicherheitsorganisation sowie Regeln und Methoden zur Gewährleistung der Informationssicherheit und Erfüllung der Norm-Anforderungen definiert.

Unter Anwendung eines Risikomanagementprozesses verleiht es interessierten Parteien Vertrauen in eine angemessene Risiko-Steuerung.

Des Weiteren leistet das DATAGROUP ISMS einen wesentlichen Beitrag zur Umsetzung und Sicherstellung datenschutzrechtlicher Anforderungen (u.a. Art. 32 DSGVO "Sicherheit der Verarbeitung personenbezogener Daten") und kann im Falle einer Datenschutzverletzung helfen, mögliche Bußgelder zu mindern.

Die Gesamtverantwortung für die Informationssicherheit hat der Vorstand.

Als oberstes Sicherheitsgremium wurde das Corporate Security Board (CSB) implementiert. Mitglieder sind die Sicherheitsverantwortlichen der Gesellschaften, Company Security Manager (CSM). Diese werden von Experten des Security Operation Center (SOC) und Security Competence Teams (SCT) beraten und bei Bedarf unterstützt.

Geleitet wird das CSB vom Chief Information Security Officer (CISO), dieser berichtet direkt an den Vorstand (CEO).

9. Werden Mitarbeiter im Bereich der Informationssicherheit unterwiesen und fortlaufend geschult?

- ☒ Ja
- ☐ Nein

10. Werden hinsichtlich der Informationssicherheit Interne Audits durchgeführt?

- ☒ Ja
- ☐ Nein

11. Wie werden die Mitarbeiter über die Gefahren beim Umgang mit Informationen und deren Verarbeitung geschult sowie sensibilisiert?

Über eine Reihe von Schulungen und Quizes, publiziert über die Schulungsplattform von G-Data. Außerdem werden regelmäßig IS-Kampagnen durchgeführt (z.B. zum Thema Phishing).

12. Existiert ein Zutrittsmanagement in Ihrem Unternehmen?

- ☒ Ja
- ☐ Nein

13. Wie ist das Unternehmen gegen äußere und umgebungsbezogene Bedrohungen geschützt?

Die Flächen der Mercoline sind in der 2. Etage, die Räumlichkeiten durch verschlossene Türen gesichert.

14. In welchem Umfang ist ein Schutz vor Schadsoftware (Viren, Würmer, usw.) im Unternehmen vorhanden?

Durch Virens Scanner auf allen Devices.

15. Wie werden die Datensicherungen (Back-Up's) erstellt sowie kontrolliert und in welchem Umfang wird die Wiederherstellung (Restores) regelmäßig getestet?

Durch den ISO-zertifizierten RZ-Dienstleister gewährleistet.

16. Wird vor Auftragsvergabe an Fremdfirmen eine Risikoanalyse der personellen u. organisatorischen Risiken durchgeführt?

- ☐ Ja
- ☒ Nein

17. Wird das Unternehmensnetzwerk durch aktuelle Firewall Standards vor Zugriff Dritter geschützt?

- ☒ Ja
- ☐ Nein

18. Inwiefern gibt es Richtlinien zum Umgang mit mobilen Datenträgern (z.B. Bänder, USB-Speichersticks, USB-Festplatten, CD's, DVD's, usw.)?

Es gibt eine Richtlinie zum Arbeiten mit mobilen Endgeräten und Speichermedien.

19. Gibt es in Ihrem Unternehmen einen Prozess zur endgültigen und sicheren Entsorgung von Computermedien?

ja

20. Welche Vorsichtsmaßnahmen werden getroffen, wenn ein elektronischer Austausch von Informationen erforderlich?

Nutzung von verschlüsselten Verbindungen.

21. Gibt es eine Leitlinie zur Anwendung kryptografischer Maßnahmen (Verschlüsselung von mobilen Systemen/ Wechseldatenträger/ E-Mail) zum Schutz von Informationen?

- ☒ Ja
- ☐ Nein

22. Inwiefern sind Maßnahmen für die Entwicklung und Aufrechterhaltung der Business Continuity (Fortführung des ordnungsgemäßen Geschäftsbetriebs) im Unternehmen eingeführt?

Die Maßnahmen sind derzeit im Aufbau.

23. Inwiefern sind Regeln und Maßnahmen für den Fernzugriff (Remote Access) auf das Unternehmensnetz definiert und umgesetzt?

Definition und Umsetzung durch die Richtlinien Kryptografie, Mobiles Arbeiten, Sicherer Betrieb und Sichere Netzwerke.

24. In wie weit wurde eine Richtlinie entwickelt, die auf die Risiken beim Arbeiten mit mobilen Computern hinweist?

S. Richtlinie Mobilgeräte und mobiles Arbeiten

25. In wie weit werden Informationen über die technischen Schwachstellen der eingesetzten Informationssysteme zeitnah beschafft, beurteilt und geeignete Maßnahmen für eine Umsetzung ergriffen (Patch-Management)?

Aktives Monitoring der Schwachstellen, Einrichtung eines SOC und aktives Patchmanagement.

26. Wie wird die Geheimhaltung bei der Zusammenarbeit mit Fremdfirmen sichergestellt?

Durch den Abschluss von NDAs.

27. Wie werden die Netzwerke verwaltet und gesteuert, damit sie vor Bedrohungen geschützt sind?

Durch Netzwerksegmentierung und Firewalls.