

Ergebnisse anzeigen

Auskunftsperson
4 Anonym

27:54
Zeit zum
Ausfüllen

1. Unternehmen *

blink.it GmbH & Co. KG

2. Ansprechpartner *

Hans-Martin Sprungk

3. Besteht bereits eine Zertifizierung nach ISO 27001? *

- ☐ Ja
- ☒ Nein

4. Existiert im Unternehmen einen namentlich benannter Informationssicherheitsbeauftragter?

- ☐ Ja
- ☒ Nein

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

- ☒ Ja
- ☐ Nein

6. Gibt es im Unternehmen eine Informationssicherheitsleitlinie?

- ☒ Ja
- ☐ Nein

7. Wie ist die Informationssicherheit im Unternehmen organisiert?

Durch Prozesse, Dokumentationen, Audits und Schulungen entsprechender Mitarbeiter.

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

- ☒ Ja
- ☐ Nein

9. Werden hinsichtlich der Informationssicherheit Interne Audits durchgeführt?

- ☒ Ja
- ☐ Nein

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

In erster Linie im Einarbeitungsprozess durch den jeweiligen Vorgesetzten und dann im laufenden Arbeitsalltag bei relevanten technischen und/oder gesetzlichen Änderungen.

11. Existiert ein Zutrittsmanagement in Ihrem Unternehmen?

- ☒ Ja
- ☐ Nein

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

Siehe unsere TOM's - sende ich separat per Mail.

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

Durch eine Reihe von Maßnahmen, sowohl technisch wie organisatorisch, z.B.:

- Firewall, um unautorisierten Zugriff auf das Netzwerk zu verhindern
- starke Passwörter
- Verwenden von ausschließlich vertrauenswürdiger Software und Anwendungen
- Beschränkung des Zugriffs auf kritische Daten und Systeme nur auf autorisierte Mitarbeiter
- Analyse von Phishing Emails
- regelmäßige Softwareupdates

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

Bei den Zyklen der Datensicherung (Backups) wird zwischen Datenbanken und binären Dateien unterschieden. Die Datenbanken umfassen alle Einstellungen, Kommentare oder andere in Textform eingebrachten Informationen in die blink.it Applikation. Binäre Dateien sind hingegen Videos, Bilder, Office-Dateien und andere auf die blink.it Applikation eingebrachten Dokumente. In beiden Fällen werden die Daten auf eigenen Maschinen in der Serverlandschaft des Anbieters gespeichert. Die Speicherart, Zyklen, Wiederherstellungs- und Aufbewahrungszeit sind den folgenden beiden Tabelle zu entnehmen.

Datenbanken
Speicherart: Export als JSON
Zyklus: Täglich
Aufbewahrung: Letzte 30 Tage
Wiederherst.: 3 Tage

Binäre Dateien
Speicherart: Redundante Speicherung
Zyklus: Fortlaufend

Speicherart: Komplettspiegelung
Zyklus: Monatlich
Aufbewahrung: Letzte 2 Monate
Wiederherst.: 7 Tage

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

- ☒ Ja
- ☐ Nein

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

- ☒ Ja
- ☐ Nein

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

Siehe unsere TOM's - sende ich separat per Mail.

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

Ja.

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

Siehe unsere TOM's - sende ich separat per Mail.

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

- ☒ Ja
- ☐ Nein

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

Siehe unsere TOM's - sende ich separat per Mail.

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

Siehe unsere TOM's - sende ich separat per Mail.

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

Mit jedem Mitarbeiter wurde eine entsprechende Richtlinie besprochen und unterzeichnet.

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

Siehe Dokument zum ISMS - sende ich separat per Mail.

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

Siehe AV-Vertrag samt Anlage - sende ich separat per Mail.

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

Siehe Dokument "Datenschutz & Datensicherheit bei blink.it" - sende ich separat per Mail.