

IT-Sicherheitskonzept nach der "GM"-Methode

1. Erstellen Sie eine Sicherheits-Leitlinie & benennen Sie einen IT-Sicherheitsbeauftragten

Muster <http://www.datenschutz-guru.de/files/Sicherheitsleitlinie%20Muster.doc>

2. Beschaffen Sie sich Unterlagen - "Bestandsanalyse"

Übersicht aller Räume

Kategorisierung erlaubt, z.B.

Serverraum
Räume der Personalabteilung
Räume, die gleiche Struktur haben, also ähnlich sind, können zusammengefasst werden. Sind z.B. alle Räume, in denen Mitarbeiter arbeiten, jeweils mit Telefon, Netzwerksteckdose und abschließbarer Tür ausgestattet, können diese zusammengefasst werden

Übersicht aller IT-Systeme

mit Standorten und installierten Betriebssystemen

Beispiele
Lohn- und Gehaltsabrechnung
Teilnehmerverwaltung
Finanzbuchhaltung
E-Mail
Terminkalender

Übersicht aller IT-Anwendungen/-Verfahren

hier bitte auch die Verfahren erfassen, bei denen Sie Daten im Auftrag verarbeiten lassen

Erfassen Sie hier bitte auch alle "Prozesse", bei denen Sie IT-Systeme durch andere Unternehmen warten lassen UND nicht ausgeschlossen ist, dass das Wartungsunternehmen Zugriff auf personenbezogene Daten erhalten kann

Netzplan

1. Zielrichtung

Bei der Organisation wird für den Einsatz der IT-Systeme nach folgendem Sicherheitskonzept verfahren:

Gewährleistet werden soll
die **Verfügbarkeit** der Systeme (z. B. Schutz vor Diebstahl, Zerstörung, Ausfallzeiten, Verlust von Datenträgern),
die **Integrität** der Software und der Daten (z. B. Schutz vor vorsätzlicher oder fahrlässiger Verfälschung von Programmen, Manipulation von Dateien),
die **Vertraulichkeit** von Daten (z. B. Schutz vor unbefugter Kenntnisnahme von Datei- inhalten).

In dem Sicherheitskonzept wird ein **hohes Sicherheitsniveau** zugrunde gelegt. Es bezieht sich auf alle in der Organisation technischen Systeme und Verfahrensabläufe, mit deren Hilfe **dienstliche Informationen** gespeichert und weiterverarbeitet werden können.

In dem Sicherheitskonzept werden ausschließlich **technische und organisatorische** Maßnahmen auf der Grundlage der in der **Bestandsaufnahme** vom ermittelten Informationen und des **IT Konzeptes** vom dargestellt. Aus Gründen der Vereinfachung ist die Auswahl der Schutzmaßnahmen für die bei der Organisation eingesetzten Verfahren **zusammenfassend** beschrieben worden. In den Verfahrensakten wird deshalb auf das Sicherheitskonzept verwiesen.

Technische und organisatorische Maßnahmen i.S.d. § 9 BDSG

Muster http://www.datenschutz-guru.de/files/Ausfuellhilfe_TOM_9_BDSG_V2.doc

3. Schreiben Sie eine Einleitung zum IT-Sicherheitskonzept, aus der sich ergibt, dass Sie die 3 Säulen ("Verfügbarkeit", "Integrität", "Vertraulichkeit") für die Informationssicherheit berücksichtigen und dass der Schutzbedarf der bei Ihnen verarbeiteten Daten in der Regel nicht nur einen niedrigen, mittleren sondern hohen Schutzbedarf hat.

4. Machen Sie die "Basisangaben" für die Verfahren nach Maßgabe der Anlage zu § 9 BDSG

5. Prüfen Sie insbesondere auch Verfahren/Prozesse, bei denen Daten im Auftrag verarbeitet oder IT-Systeme gewartet werden

Gibt es einen Auftragsdatenverarbeitungsvertrag?

Nein
Prüfen Sie den Vertrag auf Konformität mit § 11 BDSG und dokumentieren Sie dies in einem Dokument <http://www.datenschutz-guru.de/files/Checkliste%20Pruefung%20Auftragsdaten-verarbeitungsvertrag.doc>
Ja
Führen Sie 1x jährlich eine Nachprüfung durch, in dem Sie beim Auftragnehmer nach Änderungen an seinen technischen und organisatorische Maßnahmen fragen und dies dokumentieren. Außerdem sollten Sie nach sonstigen Änderungen fragen (neuer DSB, Ansprechpartner etc.)

10. Schreiben Sie das IT-Sicherheitskonzept zusammen mit folgenden Bestandteilen

a) Übernehmen Sie die entworfene Einleitung (Ziff. 3) in das Dokument

b) Es sollten dann die Unterlagen aufgeführt werden (kann auf Anlagen verwiesen werden), die Sie gemäß Ziff. 2 beschafft haben

c) Fügen Sie dann in einem nächsten Abschnitt die Angaben zu den technischen und organisatorischen Maßnahmen nach § 9 BDSG (Ziff. 4) ein.

d) Fügen Sie die Risiko-/Schwachstellenanalyse (Ziff. 6) ein

e) Fügen Sie dann die Maßnahmen ein, die Sie treffen können/wollen bzw. getroffen haben, um die Risiken zu minimieren.

f) Verweisen Sie auf die IT-Richtlinie (Ziff. 8)

g) Verweisen Sie auf den Notfallplan (Ziff. 9)

h) Das Sicherheitskonzept sollte einen "Forschreibungs"-Passus enthalten

Beispiel

Das Sicherheitskonzept ist bei jeder Änderung der aktuellen örtlichen und personellen Gegebenheiten und aus sonstigen Anlässen, die Auswirkungen auf das Sicherheitskonzept haben, fortzuschreiben und spätestens nach einem Jahr zu überprüfen.

Das Sicherheitskonzept wird mit Wirkung vom in Kraft gesetzt.

Ort, Datum und Unterschrift Leiter Organisation

Hier muss geregelt sein, was in Worst-Case-Szenarios passiert, z.B. bei Brand im Serverraum

9. Sie sollten einen Notfallplan erstellen

Muster in BSI-Standard 100-4 https://www.bsi.bund.de/cae/servlet/contentblob/471456/publicationFile/30746/standard_1004.pdf

8. Sie sollten eine IT-Richtlinie verfassen

Muster <http://www.datenschutz-guru.de/files/IT-Richtlinie.doc>

7. Beschreiben Sie die Maßnahmen zur Minimierung der Gefahren, die Sie im Rahmen der Risiko-/Schwachstellenanalyse

Es macht Sinn hier die Maßnahmen aufzutrennen:

Sicherheitsmaßnahmen auf Server-Ebene
Sicherheitsmaßnahmen auf Client-Ebene
Sicherheits-Maßnahmen für Anwender und ggf. Admins

6. Machen Sie eine Risiko-/Schwachstellenanalyse in Anlehnung an die ULD-Checklisten

Nehmen Sie erst die Prüffragen der "Checkliste" und beantworten Sie. Die Gefahrenhinweise helfen Ihnen zu einzelnen Punkten weiter

S. 50 ff. von "backup 01" <https://www.datenschutzzentrum.de/backup-magazin/backup01.pdf>