

Der **IT**-Sicherheitscheck! für Ihr Unternehmen



BeSecure IT
Datenschutz für Ihre Sicherheit



Was tun und wie es funktioniert: 30 Minuten für Ihre **Sicherheit**!

IT-Sicherheit ist ein komplexes Thema für Unternehmen – heute mehr denn je!

In 30 Minuten gibt Ihnen dieser Fragekatalog einen Überblick über den Sicherheitszustand Ihres Unternehmens und fasst die aktuell wichtigen Themen im Bereich IT-Security klar und verständlich zusammen.

Gemeinsam mit der Auswertung dieses Fragebogens erhalten Sie einen Projektleitfaden, um Ihr Unternehmen optimal zu schützen und rechtssicher aufzustellen.

SecurITy
made
in
Germany



Wussten Sie...



... dass Sie gegenüber Dritten mit Bußgeldern bis zu 20.000.000 Euro haften und dies sogar trotz GmbH-Firmierung mit Ihrem Privatvermögen! Zusätzlich können weitere Schadenersatzforderungen auf Sie zukommen!

... dass ein Datenschutzbeauftragter schon bei unter 9 Angestellten Pflicht für Sie ist, wenn Sie personenbezogene Daten geschäftsmäßig elektronisch zur Übermittlung verarbeiten!

Wenn Sie jemandem (auch unbewusst/ unbeabsichtigt) Schaden zufügen:

- Datenschutzgrundverordnung (DSGVO)
- Bundesdatenschutzgesetz (BDSG)
- Telekommunikationsgesetz (TKG)
- GmbH-Gesetz (GmbHG),
- Aktiengesetz (AktG)
- Steuerberatungsgesetz (StBerG),
- Wirtschaftsgerichtsordnung (WiPrO)

Laut Bundesdatenschutzgesetz (BDSG) muss jede Firma, auch unter 9 Angestellten (z.B. Ärzte, Steuerberater, Rechtsanwälte...) einen Datenschutzbeauftragten bestellen, wenn personenbezogene Daten geschäftsmäßig elektronisch zur Übermittlung verarbeitet werden.

... dass Vorratsdatenspeicherung werden in Kürze in Deutschland umgesetzt.

... dass personenbezogene Log-Daten nicht so einfach zum Nachweis von Taten verwendet werden dürfen:

und Betreiber von Kunden-WLANs (Flughäfen, Hotels, Gaststätten...)

Betriebsverfassungsgesetz, Arbeitsrecht und Vier-Augen-Prinzip: Nur ein Datenschutzbeauftragter und Administrator dürfen gemeinsam auf personenbezogene Log-Daten zugreifen. Die Daten müssen verschlüsselt sein oder es muss eine unterschriebene Betriebsvereinbarung vorliegen.



Analyse der strategischen IT-Sicherheit

1 Strategische Sicherheit

Bitte beantworten Sie nun die folgenden Fragen:

Antwort:

ja nein

Notizen

Hat die Geschäftsführung die IT-Sicherheitsziele formuliert und sich zu ihrer Verantwortung für die IT-Sicherheit bekannt?

Dazu zählen:

- Sind die bestehenden Richtlinien und Zuständigkeiten allen Mitarbeitern bekannt und können diese jederzeit auf diese Dokumentation zugreifen?
- Ist ein IT-Sicherheitsbeauftragter/Datenschutzbeauftragter¹ schriftlich benannt worden und ist diese Person zertifiziert?
- Gibt es einen schriftlichen Risiko-Plan, um auch bei EDV-Ausfällen arbeiten zu können?
- Wird die Wirksamkeit von IT-Sicherheitsmaßnahmen² regelmäßig überprüft?
- Sind und werden gesetzliche und/oder vertragsrechtliche Gesichtspunkte in den unternehmensweiten IT-Sicherheit berücksichtigt?

☐☐☐☐☐☐☐☐☐☐

Achtung: Auch bei Unternehmen <9 Mitarbeitern ist bei der elektronischen Verarbeitung personenbezogener Daten zum Zweck der Übermittlung ein Datenschutzbeauftragter notwendig.

Wenn ja, dann was wird dagegen unternommen?

- Werden und wie werden Verstöße gegen die IT-Security-Richtlinien in Ihrem Unternehmen geahndet?

☐☐

Was sind die Folgen für Mitarbeiter: Abmahnungen etc.

Anzahl:

☐☐



2 Operative Sicherheit

Bitte beantworten Sie nun die folgenden Fragen:

Antwort:

ja nein

Notizen

Client- und Netzwerkschutz:

- Ist auf Clients (Rechner, Server, mobile Geräte etc.) ein aktuelles Schutz-Programm (Firewall, AV-Programm) installiert?
- Ist zum Gesamtschutz für das Netzwerk ein UTM-System bestehend aus Firewall, AV, VPN-Server, Spam-Filter, Web-Filter, Intrusion Detection, Log-Server etc. installiert?
- Werden regelmäßige monatliche Reports gemacht, aus der die Unternehmensleitung ersieht: Was passiert im Netzwerk, wer

☐	☐
☐	☐
☐	☐

Beachten Sie, viele Netzwerk-Systeme (Kopierer/Drucker, Fax, Switch, spezielle Server, die Netzwerkkommunikation etc.) können nicht direkt geschützt werden, das geht nur mit einer UTM. Außerdem verfügen Sie damit gemeinsam mit dem Client-Schutz über ein zweistufiges Sicherheitssystem.

Reports, Datenschutz/Verschlüsselung:

- Gibt es ein Konzept, das beschreibt, welche Daten nach innen und nach außen (zum Internet) angeboten werden?
- Ist geregelt, auf welche Daten Angewandte zugreifen dürfen?
- Wird geloggt/reported? Wer hat was im Netzwerk gemacht und wer ist verantwortlich?
- Werden gesetzliche Aufbewahrungspflichten berücksichtigt?
- Werden personenbezogene Daten sicher verarbeitet?
- Sind die Sicherheitsmechanismen auch aktiviert?
- Werden vertrauliche Daten und gefährdete Systeme wie Notebooks ausreichend durch Verschlüsselung oder andere Maßnahmen – z. B. bei Verlust/Diebstahl – geschützt?

☐	☐
☐	☐
☐	☐
☐	☐
☐	☐
☐	☐
☐	☐

Monatliche UTM-Reports zeigen der Firmenleitung auf, was im Netzwerk los ist und wie Probleme gelöst werden können: Mitarbeiter surfen zu viel im Internet, wer macht genau was und welche Kosten verursacht das. Es gibt immer mehr Vorfälle, in denen Know-How, Vertriebsdaten, personenbezogene Daten etc. aus Firmen entwendet werden bzw. diese damit erpresst werden. Eine Vielzahl von Daten unterliegen gesetzlichen Archivierungsrichtlinien, z. B. kaufmännische Daten (Rechnungen etc.) müssen 10 Jahre aufbewahrt werden, Log-Daten unterliegen arbeitsrechtlichen bzw. dem Betriebsverfassungsschutzgesetz.

Anzahl:

☐	☐
--------------------------	--------------------------





3 Technischer Datenschutz – Teil 1

Bitte beantworten Sie nun die folgenden Fragen:

Antwort:

ja nein

Notizen

Schutz durch techn. & organisatorische Maßnahmen (TOMs):

- Erfüllen Sie bei der Verarbeitung personenbezogener Daten die folgenden Kriterien:
 - Pseudonymisierung
 - Vertraulichkeit
 - Integrität
 - Verfügbarkeit
 - Belastbarkeit
- Wurden IT-Sicherheits- bzw. Benutzerrichtlinien erstellt

☐☐

Daten können ohne zusätzliche Informationen keiner spezifischen betroffenen Person zugeordnet werden
Schutz vor unbefugter Kenntnisnahme der Daten
Gewährleistung der Echtheit, Vollständigkeit, Zurechenbarkeit, Unverfälschtheit und Gültigkeit der Daten
zeitnahe Bereitstellung von Daten, Möglichkeit zur ordnungsgemäßen Archivierung
Stabilität gegenüber Angriffen / Ausfällen

☐☐

- Haben Sie einen Serverraum?
- Sind Server sicher aufgestellt?
- Sind die Büroräume / Rechnerräume nur für befugtes Personal zugänglich?
- Ist der Zutritt zu Räumen beschränkt, in denen Datenmaterial verwahrt wird (Akten, Datenträger)?

☐☐☐☐☐☐☐☐

Zugangskontrolle (Computer):

- Sind Bildschirmeffern eingerichtet?
- Wird eine Firewall installiert, aktiviert, aktualisiert?
- Ist Software zum Schutz vor Schadsoftware installiert, aktiviert und aktualisiert?
- Wurde eine Benutzeridentifikation/Authentifizierung eingerichtet?
- Werden Anmeldevorgänge überwacht und/oder protokolliert?

☐☐☐☐☐☐☐☐☐☐

Anzahl:

☐☐



4 Technischer Datenschutz – Teil 2

Bitte beantworten Sie nun die folgenden Fragen:

Antwort:

ja nein

Notizen

Zugriffskontrolle:

- Sind unterschiedliche Zugriffsrechte eingestellt und werden diese dokumentiert?

☐☐

Weitergabekontrolle:

- Werden Daten verschlüsselt weitergegeben/versendet?
- Erfolgt eine regelmäßige Wartung und Prüfung der Datenverarbeitungssysteme?
- Wird veraltetes Equipment sicher entsorgt?
- Gibt es Beschränkungen bei Nutzung von privatem Equipment?

☐
☐☐
☐

z.B. Smartphone oder Laptop

Datenschutzverletzungen:

- Gibt es Anweisungen, wie intern mit Datenschutzverstößen umzugehen ist?
- Wird sichergestellt, dass die Meldung von Verletzungen des Schutzes personenbezogener Daten innerhalb von 72 Stunden an die Aufsichtsbehörde möglich ist?
- Wurde festgelegt, wer, wann und wie mit der Datenschutzaufsichtsbehörde kommuniziert?

☐☐☐☐☐☐

Anzahl:

☐☐

■ ■ ■ ■ ■ Wo stehen Sie?

Auswertung Ihres Unternehmens

Diese Checkliste soll Sie sensibilisieren. Sie zeigt Ihnen wesentliche Lücken in der IT-Sicherheit und dem Technischen Datenschutz im Unternehmen auf und hilft Ihnen eine angemessene Lösung zu finden.

Grundsätzlich sollten Sie alle Fragen in allen Bereichen der Checkliste mit „JA“ beantworten, nur dann können Sie sicher sein, dass Sie auf dem richtigen Weg sind!

Diese strukturierte Vorgehensweise und das Feststellen des Bedarfs in IT-Sicherheit und Datenschutz soll Ihnen einerseits die Gewissheit geben das Optimale zu tun, aber auch klar aufzeigen:

„Wo sind die Schwächen, was ist wichtig, was muss getan werden und steht alles in einem vernünftigen Kosten-/Nutzenverhältnis!“

