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!

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

- Datenschutzgrundverordnung (DSGVO)
- Bundesdatenschutzgesetz (BDSG)
- Telekommunikationsgesetz (TKG)
- GmbH-Gesetz (GmbHG),
- Aktiengesetz (Akt
- Steuerberatun gese StBerG),
- Wirtschafts erordnu g (WiPrO)

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

Laut Bundesda utzgesetz (BDSG) muss jede Firma, ch unter 9 Angestellten (z.B. Ärzte, Steuerbe r, Rechtsanwälte…) einen Datenschutzbeauftragten bestellen, wenn ersonenbezogene Daten geschäfts- m g elektronisch zur Übermittlung erarbeitet rden.

… Vorratsdatenspeicherung werden in Kürze in Deutschland umgesetzt.

und Betreiber von Kunden-WLANS (Flughäfen, Hotels, Gaststätten…)

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

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.

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/Datenschutzbeauftragter[1] schriftlich benannt worden und ist dieser qualifiziert?	☐ ☐	**Achtung:** Auch bei Unternehmen <9 Mitarbeitern ist bei der elektronischen Verarbeitung personenbezogener Daten zum Zweck der Übermittlung ein Datenschutzbeauftragter notwendig.
• Gibt es einen schriftlichen Risiko-Plan, um auch bei EDV-Ausfällen arbeiten zu können?	☐ ☐	
• Wird die Wirksamkeit von IT-Sicherheitsmaßnahmen[2] regelmäßig überprüft?	☐ ☐	
• Sind und werden gesetzliche und/oder vertragsrechtliche Gesichtspunkte in den Unternehmensbereichen IT-Sicherheit berücksichtigt?	☐ ☐	
• 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?	☐	☐	Beachten Sie, viele Netzwerk-Systeme (Kopierer/Drucker, Faxe, Switche, spezielle Server, die Netzwerkkommunikation etc.) können nicht direkt geschützt werden, das geht nur mi[illegible]ner UTM. Außerdem verfügen [illegible] dami[illegible]emeinsam mit dem Clients[illegible]tz übe[illegible] ein zweistufiges Sich[illegible]eitssystem.
• 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	☐	☐	
Reports, Datenschutz/Verschlüsselung: • Gibt es ein Konzept, das beschreibt, welche Dat[illegible]n na[illegible]innen und nach außen (zum Internet) angeboten werden?	☐	☐	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 gibts 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 Betriebsverfassungsschutzgesetzen.
• Ist geregelt, auf welche Daten An[illegible]der zugreifen dürfen?	☐	☐	
• Wird geloggt/reporte[illegible] Wer hat was i[illegible]letzwerk gemacht und wer ist verantwortlich?	☐	☐	
• Werden gesetzliche Aufbe[illegible]hrungspf[illegible]nten berücksichtigt?	☐	☐	
• Werden p[illegible]sonenbezogene [illegible][illegible]ner verarbeitet?	☐	☐	
• Sind die S[illegible]heitsmechanismen auch aktiviert?	☐	☐	
• Werden ver[illegible]au[illegible]he Daten und gefährdete Systeme wie Notebooks a[illegible]reic[illegible]nd durch Verschlüsselung oder andere [illegible]hmen – z. B. b[illegible] Verlust/Diebstahl – geschützt?	☐	☐	
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	☐	☐	Daten können ohne zusätzliche Informationen keiner spezifischen betroffenen Person zugeordnet werden Schutz vor unbe… Kenntnisnahme der Daten Gewährleis…g der Ec…it, Vollständigkeit, Zurechenbarkeit, l…beherrschaft u… Gültigkeit der Daten zeitg…nte Bereitstell…g von Daten, Möglichkeit zur ordn…gemäßen R… Stabilität …enüb… Angriffen / Ausfällen
• Wurden IT-Sicherheits- bzw. Benutzerrichtlinien erstellt	☐	☐	
- Haben Sie einen Serverraum?	☐	☐	
- Sind Server sich… aufgestellt?	☐	☐	
• Sind die Büroräume /…chnerräume nur für befugtes Personal zugänglich?	☐	☐	
• Ist der Zutritt zu Räumen be…kt, in denen Datenmaterial verwah…d (Akten, Datenträger)?	☐	☐	
Zugangsko…troll…n (Computer):			
• Sind Bildsc…irms…rren eingerichtet?	☐	☐	
• …de eine Firewa…nstalliert, aktiviert, aktualisiert?	☐	☐	
• …Soft…re z…m Schutz vor Schadsoftware installiert, aktiviert und …ktualisi…	☐	☐	
• Wurd…ine 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? • Ist 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 vernünftigem Kosten-/Nutzenverhältnis!“