

## Die 4x4 Fragen zur IT-Sicherheit in Ihrem Unternehmen

Der folgende Kurz-Check vermittelt Ihnen einen ersten Überblick über den Stand der Informationssicherheit in Ihrem Unternehmen bzw. in Ihrer Organisation. Die Auswertung der Fragen gibt Ihnen Hinweise auf den Handlungsbedarf zur kurzfristigen Erhöhung Ihrer IT-Sicherheit. Anleitungen zu konkreten Schritten finden Sie auf der Rückseite.

	<i>Ja</i>	<i>Nein</i>
<b>I Management der IT-Sicherheit</b>		
• Existiert in Ihrem Unternehmen eine übergreifende IT-Sicherheitspolitik / -strategie?	<input type="checkbox"/>	<input type="checkbox"/>
• Sind Ihre geschäftskritischen Informationen/Daten vollständig klassifiziert? Werden vertrauliche Informationen sicher übermittelt?	<input type="checkbox"/>	<input type="checkbox"/>
• Werden Sicherheitsvorfälle im Unternehmen analysiert? Sind Sie über den aktuellen Stand der IT-Sicherheit umfassend informiert?	<input type="checkbox"/>	<input type="checkbox"/>
• Haben Sie einen festen Ansprechpartner für Sicherheitsfragen benannt, der allen Mitarbeitern bekannt und für diese erreichbar ist?	<input type="checkbox"/>	<input type="checkbox"/>
<b>II Technik</b>		
• Sichern Sie geschäftskritische Daten regelmäßig? Lagern Sie die Sicherungen aus? Werden Sicherungsmedien und Recovery-Prozeduren auf Funktionsfähigkeit überprüft?	<input type="checkbox"/>	<input type="checkbox"/>
• Nutzen Sie Anti-Virus Programme und werden diese regelmäßig aktualisiert?	<input type="checkbox"/>	<input type="checkbox"/>
• Werden sicherheitsrelevante Programmkorrekturen (Patches) auf allen Systemen tagesaktuell eingespielt?	<input type="checkbox"/>	<input type="checkbox"/>
• Sind Server bzw. Serverräume gegen Zugriff bzw. Zutritt von nicht autorisierten Personen ausreichend geschützt?	<input type="checkbox"/>	<input type="checkbox"/>
<b>III Organisation</b>		
• Existieren betriebsinterne Richtlinien und Anweisungen für E-Mail und Internet-Nutzung oder den Umgang mit Passwörtern?	<input type="checkbox"/>	<input type="checkbox"/>
• Existieren betriebsinterne Richtlinien oder Anweisungen für den Betrieb der IT-Infrastruktur (Richtlinien für Administratoren bzw. externe Dienstleister)?	<input type="checkbox"/>	<input type="checkbox"/>
• Sind Ihre Mitarbeiter auf die Inhalte der Sicherheitsrichtlinie geschult?	<input type="checkbox"/>	<input type="checkbox"/>
• Existieren Notfallpläne für den Schadensfall (z.B. Verlust geschäftskritischer Daten, Virusbefall oder Brand)? Sind alle Mitarbeiter über richtiges Verhalten in Notfällen informiert?	<input type="checkbox"/>	<input type="checkbox"/>
<b>IV Datenschutz</b>		
• Werden in Ihrem Unternehmen personenbezogene Daten verarbeitet?	<input type="checkbox"/>	<input type="checkbox"/>
• Sind mehr als vier Personen an der elektronischen Verarbeitung der personenbezogener Daten beteiligt?	<input type="checkbox"/>	<input type="checkbox"/>
• Hat Ihr Unternehmen einen Datenschutzbeauftragten bestellt?	<input type="checkbox"/>	<input type="checkbox"/>
• Werden die datenschutzrechtlichen Bestimmungen in Bezug auf Datenerhebung, -verarbeitung, -nutzung und -übermittlung eingehalten?	<input type="checkbox"/>	<input type="checkbox"/>



## I Management der Informationssicherheit

- Etablieren Sie eine umfassende Sicherheitspolitik sowie ein Sicherheits-Management in Ihrem Unternehmen.
- Ihr Wissen um geschäftskritische Informationen ist die Basis für wirksame Sicherheitsmaßnahmen. Verschaffen Sie sich vollständige Klarheit über das schützenswerte Gut Ihres Unternehmens.
- Führen Sie eine detaillierte Analyse der IT-Sicherheit und -Risiken im Unternehmen durch.
- Benennen Sie ein Sicherheits-Management-Team mit klar definierten Rollen und Verantwortlichkeiten im Unternehmen und informieren Sie die Mitarbeiter darüber.

## II Technische Maßnahmen

- Etablieren Sie ein zuverlässiges Datensicherungssystem, das regelmäßig durch Testläufe überprüft wird.
- Erarbeiten Sie ein Viren-Schutz-Konzept und setzen Sie dieses auf allen PCs und Servern im Unternehmen in die Praxis um. Achten Sie auf fortlaufende Aktualität.
- Spielen Sie sicherheitsrelevante Patches schnellstens ein. Erarbeiten Sie für kritische Systeme Test- und Rückfallszenarien, um Ihren Betrieb möglichst nicht zu gefährden.
- IT-Betriebsräume müssen vor unbefugtem Zugriff geschützt werden. Der Zutritt z.B. zu Serverräumen sollte auf autorisierte Personen beschränkt sein.

## III Organisatorische Maßnahmen

- Eine firmenübergreifende Sicherheitsrichtlinie ist die Basis für ein korrektes Verhalten der Mitarbeiter. Existiert diese bereits, überprüfen Sie sie auf Aktualität und gesetzliche Konformität und passen Sie sie ggf. an.
- Verhaltensanweisungen für Mitarbeiter im IT-Betrieb (Administratoren, Entwickler, etc.) legen Sie idealerweise in einer weiteren, technisch detaillierteren Sicherheitsrichtlinie fest.
- Informieren Sie Ihre Mitarbeiter durch Schulungen /Trainings oder andere Sensibilisierungsmaßnahmen über die in der Sicherheitsrichtlinie festgeschriebenen Regelungen und Vorgaben.
- Notfallhandbücher sollten ebenso selbstverständlich sein wie Fluchtpläne. Informieren Sie Ihre Mitarbeiter über Inhalt und Aufbewahrungsort.

## IV Maßnahmen zum Datenschutz

- Die Verarbeitung persönlicher Daten unterliegt den gesetzlichen Bestimmungen des Bundesdatenschutzgesetzes (BDSG).
- Sobald mehr als 4 Personen personenbezogene Daten in elektronischer Form verarbeiten, ist laut Gesetz ein Datenschutzbeauftragter zu bestellen.
- Eine pro forma- oder Nicht-Bestellung des Datenschutzbeauftragten kann erhebliche Geldbußen nach sich ziehen. Der DSB kann ein interner Mitarbeiter, aber auch ein externer Dienstleister sein.
- Durch Bestellung eines DSB und Schulung der Mitarbeiter vermeiden Sie Verstöße gegen das Datenschutzgesetz. Für evtl. Schäden aus der Verletzung datenrechtlicher Bestimmungen haftet das Unternehmen/der Geschäftsführer.