protekto
Für den Menschen

Checkliste
Wie sicher ist Ihre IT-Sicherheit?

Die folgende Checkliste fasst die wichtigsten IT-Sicherheitsanforderungen und -maßnahmen in kurzen Fragen zusammen, die Sie nur mit Ja, Nein oder Prüfen zu beantworten brauchen. Anhand Ihrer Antworten erhalten Sie ein sehr genaues Bild über den aktuellen Zustand der IT-Sicherheit in Ihrem Unternehmen. Die Checkliste entspricht den Sicherheitskriterien, die im IT-Grundschutzkatalog festgelegt sind, das vom Bundesamt für die Sicherheit in der Informationstechnik (BSI) herausgegeben wird (www.bsi.bund.de). Aus Gründen der besseren Lesbarkeit findet in dieser Checkliste ausschließlich das generische Maskulinum Verwendung, das als geschlechtsneutral verstanden werden soll.

1. Sicherheitsmanagement	Ja	Nein	Prüfen
Hat die Unternehmensleitung verbindliche IT-Sicherheitsziele festgelegt und die eigene Verantwortung für die IT-Sicherheit ebenfalls ausdrücklich schriftlich fixiert?			
Gibt es einen IT-Sicherheitsbeauftragten?			
Wurde der IT-Sicherheitsbeauftragte angemessen geschult?			
Muss ein Datenschutzbeauftragter bestellt werden?			
Wird der Datenschutzbeauftragte in die Entscheidungsprozesse für die Festlegung der Sicherheitsmaßnahmen eingebunden?			
Werden bei der Planung und Umsetzung der Sicherheitsmaßnahmen alle erforderlichen gesetzlichen Rahmenbedingungen beachtet?			
Ist in der Planung berücksichtigt worden, ob die Sicherheitsmaßnahmen einmalig oder regelmäßig durchgeführt werden müssen?			
Gibt es einen Terminplan für die Überprüfung der Sicherheitsmaßnahmen?			
Gibt es eine Liste, in der die Zuständigkeiten und Verantwortlichkeiten für die Umsetzung der IT-Sicherheitsmaßnahmen festgelegt sind?			
Sind die notwendigen Passwörter so hinterlegt, dass notfalls auch andere Mitarbeiter die Sicherheitsmaßnahmen durchführen können?			
Sind die bestehenden Sicherheitsrichtlinien und Zuständigkeiten allen Mitarbeitern bekannt, die mit der Durchführung von Sicherheitsmaßnahmen betraut sind?			
Werden IT-Sicherheitserfordernisse bei neuen Projekten, insbesondere bei der Planung von Netzwerkerweiterungen, Neuanschaffungen von Computer- und Kommunikationssystemen sowie IT- Dienstleistungserträgen, frühzeitig berücksichtigt?			
Gibt es Checklisten, in denen genau aufgeführt ist, was in Bezug auf die IT-Sicherheit beim Eintritt neuer Mitarbeiter und beim Ausscheiden von Mitarbeitern zu beachten ist (Kennwörter, Berechtigungen, Schlüssel/Zutrittssysteme usw.)?			
Wird die Wirksamkeit der IT-Sicherheitsmaßnahmen regelmäßig überprüft?			
Ist das IT-Sicherheitskonzept dokumentiert und steht es allen Mitarbeitern zur Verfügung?			
Gibt es IT-Sicherheitsrichtlinien, die jedem Mitarbeiter ausgehändigt werden?			

protekto
Für den Menschen

2. Allgemeine Sicherheitsaspekte und Verhalten in Notfällen	Ja	Nein	Prüfen
Viele Programme und IT-Anwendungen sind bereits mit bestimmten Schutzmechanismen ausgestattet. Werden diese Schutzmechanismen genutzt?			
Werden Virenschutzprogramme flächendeckend eingesetzt und ständig aktualisiert?			
Sind Firewall-Lösungen vorhanden und werden diese eingesetzt?			
Sind allen Benutzern der IT-Systeme Benutzernamen, Kennwörter und bestimmte Rechte bzw. Rollen und Profile zugeteilt worden?			
Gibt es Zugriffsbeschränkungen und ist klar geregelt, auf welche Daten jeder Mitarbeiter zugreifen darf?			
Gibt es auch für Administratoren unterschiedliche Zugriffsrechte und/oder unterschiedliche Rollen und Profile?			
Ist geregelt, welche Rechte und Privilegien Programme/Applikationen und Benutzer innerhalb der Systeme haben?			
Werden bei IT-Komponenten die werkseitigen Standardeinstellungen für Benutzernamen und Kennwörter geändert und angepasst?			
Werden sicherheitsrelevante Programme und Funktionen, die nicht benötigt werden, tatsächlich deinstalliert und deaktiviert?			
Wissen alle Benutzer, wie sie sicherheitskonform handeln und Risiken beim Internetzugriff sowie beim Empfangen und Versenden von E-Mails vermeiden?			
Wissen alle Benutzer, wie sie sich verhalten sollten, wenn ein Virenschutzprogramm einen Schadprogrammbefall meldet?			
Gibt es aktuelle schriftliche Handlungsanweisungen für die sicherheitskonforme IT-Nutzung?			
Werden ausführliche Installations- und Systemdokumentationen erstellt und regelmäßig aktualisiert?			
Gibt es einen Notfallplan für alle wichtigen Notfallsituationen, der außer detaillierten Verhaltensanweisungen auch Namen und Kontaktangaben von Verantwortlichen und Ansprechpartnern enthalt?			
Werden die angegebenen Handlungsanweisungen und Kontaktadressen regelmäßig überprüft und aktualisiert?			
Wissen alle Mitarbeiter, dass es einen Notfallplan gibt, und wie dieser zugänglich ist?			

3. Sicherheitsbewusstsein	Ja	Nein	Prüfen
Werden alle Benutzer und alle Beschäftigten regelmäßig in Fragen der IT-Sicherheit und des Datenschutzes unterwiesen?			
Sind alle Mitarbeiter mit den Grundsätzen des rechtskonformen Umgangs mit personenbezogenen Daten vertraut?			
Werden vertrauliche Informationen und Datenträger mit vertraulichen Informationen sorgfältig aufbewahrt und zusätzlich geschützt (verschlüsselt)?			

protekto
Für den Menschen

Erhalten alle Mitarbeiter einen Sicherheitsleitfaden, in deM sämtliche sicherheitsrelevante Themen und ein Verhaltenskodex enthalten sind?			
Werden vertrauliche Informationen vor Wartungs- und Reparaturarbeiten von Datenträgern und IT-Systemen, die Mitarbeitern von Fremdfirmen zugänglich sein könnten, entfernt und gelöscht?			
Gibt es weitere Maßnahmen, die das Sicherheitsbewusstsein der Mitarbeiter erhöhen sollen?			
Werden die bestehenden Sicherheitsvorgaben kontrolliert und Verstöße dagegen geahndet?			

4. Benutzernamen, Kennwörter und Verschlüsselung	**Ja**	**Nein**	**Prüfen**
Werden die Sicherheitsmechanismen der eingesetzten Programme genutzt und sind Sicherheitsmechanismen wie Passwortschutz oder Verschlüsselung vorhanden und aktiviert?			
Ist sichergestellt, dass voreingestellte oder leere Pass- und Kennwörter geändert wurden?			
Gibt es Vergaberichtlinien für Benutzernamen sowie Pass- und Kennwörter?			
Werden Benutzernamen und Pass- und Kennwörter zentral dokumentiert?			
Wenn Mitarbeiter selbst Pass- und Kennwörter vergeben: Sind alle Mitarbeiter in der Vergabe sicherer Kennwörter geschult und werden auch die selbst vergebenen Kennwörter zentral dokumentiert?			
Werden Arbeitsplatzrechner mit Bildschirmschoner und dazugehörigem Kennwort gesichert und vor neugierigen Blicken geschützt?			
Werden vertrauliche Daten und besonders gefährdete Systeme (z. B. Notebooks und andere mobile Informationssysteme) durch Verschlüsselung geschützt?			
Ist gewährleistet, dass vertrauliche Daten per E-Mail verschlüsselt übertragen werden?			
Werden Computer, auf denen sich sicherheitsrelevante Daten befinden, durch zusätzliche Sicherheitsmaßnahmen geschützt?			
Erfolgt der externe Zugriff auf das lokale Firmennetzwerk über getunnelte und durch Verschlüsselung gesicherte VPN-Verbindungen?			

5. Internet und E-Mail	**Ja**	**Nein**	**Prüfen**
Gibt es eine Firewall?			
Wird die Konfiguration der Firewall regelmäßig kontrolliert und aktualisiert?			
Ist festgelegt, welche Daten übers Internet angeboten/verschickt werden dürfen?			
Ist festgelegt, wie mit sicherheitsgefährdenden Zusatzprogrammen (PlugIns) und aktiven Inhalten (z. B. ActiveX) umgegangen wird?			
Sind alle unnötigen Dienste und Programmfunktionen deaktiviert?			

protekto
Für den Menschen

Sind Web-Browser und E-Mail-Programme sicher konfiguriert?			
Sind die Mitarbeiter ausreichend für die Internetnutzung und den E-Mail-Einsatz geschult?			
Gibt es verbindliche Richtlinien für die Nutzung des Internets?			
Gibt es eine E-Mail-Sicherheitsrichtlinie?			
Gibt es Vorkehrungen gegen Spam-Mails (z. B. Filter)?			
Wissen alle Benutzer, wie sie mit den Spam-Mails, die trotz der Spam-Filter in den Posteingang gelangen, umgehen sollen?			
Sind alle Mitarbeiter über Phishing-Attacken informiert und wissen sie, wie sie sich in Bezug auf Phishing-Mails zu verhalten haben?			
Gibt es eine Regelung für privates Surfen und private E-Mail-Korrespondenz?			

6. Datensicherung	**Ja**	**Nein**	**Prüfen**
Gibt es einen Plan für die zentrale Datensicherung?			
Gibt es feste Verantwortlichkeiten für die Durchführung der zentralen Datensicherung?			
Ist festgelegt, welche Daten wie lange gesichert werden?			
Ist berücksichtigt, dass die Daten in mehreren Sicherungssätzen gesichert und ältere Sicherungen mit neueren Sicherungen überschrieben werden?			
Werden die Sicherungssätze an unterschiedlichen Orten innerhalb und außerhalb des Unternehmens verteilt aufbewahrt?			
Erfolgt die externe Sicherung der Daten über eine sichere Internetverbindung?			
Werden wichtige Daten täglich gesichert?			
Ist eine schnelle Rücksicherung der Daten möglich?			
Werden die Sicherungsdatenträger regelmäßig kontrolliert?			
Sind die Sicherungs- und Rücksicherungsverfahren dokumentiert?			
Sind die Mitarbeiter verpflichtet, regelmäßig Sicherungen ihrer eigenen Dokumente vorzunehmen, und sind sie mit der Wiederherstellung der Daten vertraut?			

7. Drahtlose Netzwerkverbindungen (WLAN) und Hotspots	**Ja**	**Nein**	**Prüfen**
Ist die Außenreichweite der WLAN-Access-Points bekannt?			
Wurden bei WLAN-Access-Points und WLAN-Routern die werkseitig eingestellten Kennwörter geändert?			
Sind die WLAN-Verbindungen mit einem speziellen Netzwerkkennwort (SSID) gesichert?			

protekto
Für den Menschen

Ist auf den WLAN-Komponenten die WPA2-Verschlüsselung aktiviert?			
Sind auf den WLAN-Access-Points und -Routern die MAC-Adressen der zugelassenen WLAN-Adapter eingetragen?			
Sind zusätzliche Authentifizierungsmechanismen aktiviert?			

8. Software-Nutzung und Software-Updates	**Ja**	**Nein**	**Prüfen**
Gibt es einen Verantwortlichen für Sicherheits-Updates?			
Werden Sicherheits-Updates regelmäßig eingespielt?			
Sind Benutzer verpflichtet, Sicherheits- und Windows-Updates selbst durchzuführen?			
Wird die Durchführung der Software-Updates regelmäßig überprüft?			
Werden Updates für Anwendungsprogramme getestet, bevor sie für die allgemeine Verwendung freigegeben werden?			
Wurden alle Benutzer darauf hingewiesen, dass Programme aus dem Internet nur nach ausdrücklicher Genehmigung des Administrators heruntergeladen und installiert werden dürfen?			
Ist es den Benutzern ausdrücklich untersagt worden, eigene Programme auf den Firmen-PCs zu installieren?			

9. Schutzvorkehrungen und Schutzeinrichtungen	**Ja**	**Nein**	**Prüfen**
Sind die Server der IT-Systeme ausreichend gegen Feuer, Überhitzung und Wasserschäden geschützt?			
Sind die Server und wichtige Arbeitsplatzrechner gegen Überspannungen und Stromausfall geschützt?			
Ist der Zutritt zu wichtigen Teilen der IT und den Serverräumen geregelt?			
Gibt es eine Eingangskontrolle?			
Müssen Besucher, Handwerker und andere externe Dienstleister beaufsichtigt werden?			
Gibt es Überwachungskameras?			
Ist das Firmengelände gegen unbefugtes Betreten gesichert?			
Besteht ein ausreichender Schutz vor Einbrechern?			
Werden Firmengelände und Firmengebäude nachts von einem Wachdienst kontrolliert?			
Ist der Bestand von Hard- und Software in einer Inventarliste erfasst und werden regelmäßige Bestandskontrollen durchgeführt?			
Sind wichtige Geräte durch zusätzliche Maßnahmen geschützt, die einen Sicherheitsalarm auslösen, wenn diese unbefugt genutzt werden?			