Fragenkatalog nach IT-Grundschutz – Bundesamt für Sicherheit in der Informationstechnik

IT-Sicherheitsmanagement	
1	Hat die Unternehmens- bzw. Behördenleitung die IT-Sicherheitsziele festgelegt und sich zu ihrer Verantwortung für die IT-Sicherheit bekannt? Sind alle gesetzlichen oder vertragsrechtlichen Gesichtspunkte berücksichtigt worden?
2	Gibt es einen IT-Sicherheitsbeauftragten?
3	Werden IT-Sicherheitserfordernisse bei allen Projekten frühzeitig berücksichtigt (z. B. bei Planung eines neuen Netzes, Neuanschaffungen von IT-Systemen und Anwendungen, Outsourcing- und Dienstleistungsverträgen)?
4	Besteht ein Überblick über die wichtigsten Anwendungen und IT-Systeme und deren Schutzbedarf?
5	Gibt es einen Handlungsplan, der Sicherheitsziele priorisiert und die Umsetzung der beschlossenen IT-Sicherheitsmaßnahmen regelt?
6	Ist bei allen IT-Sicherheitsmaßnahmen festgelegt, ob sie einmalig oder in regelmäßigen Intervallen ausgeführt werden müssen (z. B. Update des Viren-Schutzprogramms)?
7	Sind für alle IT-Sicherheitsmaßnahmen Zuständigkeiten und Verantwortlichkeiten festgelegt?
8	Gibt es geeignete Vertretungsregelungen für Verantwortliche und sind die Vertreter mit ihren Aufgaben vertraut? Sind die wichtigsten Passwörter für Notfälle sicher hinterlegt?
9	Sind die bestehenden Richtlinien und Zuständigkeiten allen Zielpersonen bekannt?
10	Gibt es Checklisten, was beim Eintritt neuer Mitarbeiter und beim Austritt von Mitarbeitern zu beachten ist (Berechtigungen, Schlüssel, Unterweisung etc.)?
11	Wird die Wirksamkeit von IT-Sicherheitsmaßnahmen regelmäßig überprüft?
12	Gibt es ein dokumentiertes IT-Sicherheitskonzept?

Sicherheit von IT-Systemen	
13	Werden vorhandene Schutzmechanismen in Anwendungen und Programmen genutzt?
14	Werden flächendeckend Viren-Schutzprogramme eingesetzt?
15	Sind allen Systembenutzern Rollen und Profile zugeordnet worden?
16	Ist geregelt, auf welche Datenbestände jeder Mitarbeiter zugreifen darf? Gibt es sinnvolle Beschränkungen?
17	Gibt es verschiedene Rollen und Profile für Administratoren oder darf jeder Administrator alles?
18	Ist bekannt und geregelt, welche Privilegien und Rechte Programme haben?
19	Werden sicherheitsrelevante Standardeinstellungen von Programmen und IT-Systemen geeignet angepasst oder wird der Auslieferungszustand beibehalten?
20	Werden nicht benötigte sicherheitsrelevante Programme und Funktionen konsequent deinstalliert bzw. deaktiviert?
21	Werden Handbücher und Produktdokumentationen frühzeitig gelesen?
22	Werden ausführliche Installations- und Systemdokumentationen erstellt und regelmäßig aktualisiert?

Gefördert durch:

Bundesministerium für Wirtschaft und Energie

aufgrund eines Beschlusses des Deutschen Bundestages

Mittelstand-Digital

Vernetzung und Internet-Anbindung	
23	Gibt es eine Firewall?
24	Werden Konfiguration und Funktionsfähigkeit der Firewall regelmäßig kritisch überprüft und kontrolliert?
25	Gibt es ein Konzept, welche Daten nach außen angeboten werden müssen?
26	Ist festgelegt, wie mit gefährlichen Zusatzprogrammen (PlugIns) und aktiven Inhalten umgegangen wird?
27	Sind alle unnötigen Dienste und Programmfunktionen deaktiviert?
28	Sind Web-Browser und E-Mail-Programm sicher konfiguriert?
29	Sind die Mitarbeiter ausreichend geschult?

Beachtung von Sicherheitserfordernissen	
30	Werden vertrauliche Informationen und Datenträger sorgfältig aufbewahrt?
31	Werden vertrauliche Informationen vor Wartungs-oder Reparaturarbeiten von Datenträgern oder IT-Systemen gelöscht?
32	Werden Mitarbeiter regelmäßig in sicherheitsrelevanten Themen geschult?
33	Gibt es Maßnahmen zur Erhöhung des Sicherheitsbewusstseins der Mitarbeiter?
34	Werden bestehende Sicherheitsvorgaben kontrolliert und Verstöße geahndet?

Wartung von IT-Systemen: Umgang mit Updates	
35	Werden Sicherheits-Updates regelmäßig eingespielt?
36	Gibt es einen Verantwortlichen, der sich regelmäßig über Sicherheitseigenschaften der verwendeten Software und relevanter Sicherheits-Updates informiert?
37	Gibt es ein Testkonzept für Softwareänderungen?

Passwörter und Verschlüsselung	
38	Bieten Programme und Anwendungen Sicherheitsmechanismen wie Passwortschutz oder Verschlüsselung? Sind die Sicherheitsmechanismen aktiviert?
39	Wurden voreingestellte oder leere Passwörter geändert?
40	Sind alle Mitarbeiter in der Wahl sicherer Passwörter geschult?
41	Werden Arbeitsplatzrechner bei Verlassen mit Bildschirmschoner und Kennwort gesichert?
42	Werden vertrauliche Daten und besonders gefährdete Systeme wie Notebooks ausreichend durch Verschlüsselung oder andere Maßnahmen geschützt?

Notfallvorsorge	
43	Gibt es einen Notfallplan mit Anweisungen und Kontaktadressen?
44	Werden alle notwendigen Notfallsituationen behandelt?
45	Kennt jeder Mitarbeiter den Notfallplan und ist dieser gut zugänglich?

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages
Mittelstand-Digital

Datensicherung	
46	Gibt es eine Backupstrategie?
47	Ist festgelegt, welche Daten wie lange gesichert werden?
48	Bezieht die Sicherung auch tragbare Computer und nicht vernetzte Systeme mit ein?
49	Werden die Sicherungsbänder regelmäßig kontrolliert?
50	Sind die Sicherungs- und Rücksicherungsverfahren dokumentiert?

Infrastruktursicherheit	
51	Besteht ein angemessener Schutz der IT-Systeme gegen Feuer, Überhitzung, Wasserschäden, Überspannung und Stromausfall?
52	Ist der Zutritt zu wichtigen IT-Systemen und Räumen geregelt? Müssen Besucher, Handwerker, Servicekräfte etc. begleitet bzw. beaufsichtigt werden?
53	Besteht ein ausreichender Schutz vor Einbrechern?
54	Ist der Bestand an Hard- und Software in einer Inventarliste erfasst?

Zusätzliche Fragen	
A	Mobile Endgeräte (Smartphones, Tablets) Dort befinden sich mittlerweile auch Daten (Mails …) darauf, die sicherheitsrelevant sind. Sind diese Geräte (das können firmeneigene oder BYOD Geräte sein) mit einer Antivirensoftware ausgestattet und könnten diese bei Bedarf von extern gesperrt werden?
B	Firewall Wie wird mit Updates und Patches verfahren? Gibt es Regelungen?
C	Updates von Antivirensoftware sollte automatisiert erfolgen. Wie wird kontrolliert, ob die Software auch überall aktuell ist?
D	Updates Kritische Updates von Microsoft, Adobe, Browsern etc. – sollte automatisiert verteilt werden – hier Stichpunkt: Patch-Management
E	Datensicherung: Existiert die 3-2-1 Regel? Ein aktueller Datenträger sollte sich außerhalb der Firmenräume befinden, Nutzung von Backup in ein deutsches Rechenzentrum
F	E-Mail-Verkehr: Werden generell nur verschlüsselte Mails versandt oder bei Bedarf?
G	Wie kann ein Hackerangriff von der Firma erkannt werden?
H	Gibt es mit externen IT-Dienstleistern eine ADV (automatische Datenverarbeitung)?

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages
Mittelstand-Digital