Selbstcheck- Fragenkatalog auf Basis VdS 10000

COMPACT GmbH
Gesellschaft für Informationstechnologie

Nr.	Frage	JA	NEIN
1	**Hat die Unternehmensführung sich schriftlich verpflichtet, die Gesamtverantwortung für die Informationssicherheit wahrzunehmen?** (Erstellen einer Leitlinie als zentrales Dokument für den Informationssicherheitsprozess, definiert Ziele und Stellenwert im Unternehmen, Aufgaben und Konsequenzen bei Nichtbeachtung)		
2	**Sind klare Verantwortlichkeiten definiert?** (jedem Verantwortlichen müssen Aufgaben und Pflichten klar sein)		
3	**Ist das Prinzip der Funktionstrennung umgesetzt? (Ausführung / Kontrolle)** (Widersprüchliche Verantwortlichkeiten dürfen nicht von ein und derselben Person wahrgenommen werden)		
4	**Sind Richtlinien für die Mitarbeiter im Umgang mit der IT und den Daten definiert?** (generelle Nutzungsbedingungen, Privatnutzung, Verhaltensregeln für Hard- und Softwareinstallation, mobile Datenträger, Zugangskennungen, Datenübertragung, Abwesenheitsregelung, Missbrauchskontrolle /Protokollierung, Festlegung von begründeten Ausnahmen)		
5	**Ist die private Nutzung der Unternehmens-IT geregelt?** (Rechte und Pflichten, Kontrollmöglichkeiten durch Arbeitgeber, Einhaltung/ Verweis auf Datenschutz bzw. Einschränkung der Persönlichkeitsrechte)		
6	**Wurde eine Richtlinie für den IT-Dienstleister definiert?** **Ist die Systemdokumentation vor Ort und aktuell?** (generelle Nutzung im Supportfall, Umgang mit zur Kenntnis gelangten Daten, Einrichtung von Netzzugängen zum Zugriff, Verträge, Missbrauchskontrolle)		
7	**Kennen alle internen und externen Mitarbeiter die betreffenden Regelungen zur Informationssicherheit? Haben alle eine Vertraulichkeitserklärung abgegeben?** (Regelmäßige, nachweisliche Schulung und Sensibilisierung, zeitnahe Auswertung von Sicherheitsvorfällen, Erklärung auch über die Dauer des Arbeitsverhältnisses hinaus)		
8	**Werden alle internen und externen Mitarbeiter regelmäßig über die Maßnahmen zur Informationssicherheit informiert?** (zielgruppenorientiert über Gefährdungen, Wissenstest)		
9	**Werden Zugänge konsequent nur gewährt, wenn sie zur Aufgabenerfüllung notwendig sind? Sind die administrativen Zugänge ausschließlich den Administratoren vorbehalten?** (Beantragung und Prüfung von Zugängen, Rechteverwaltung gemäß Aufgabenverteilung, nur in begründeten Fällen Vergabe von administrativen Zugängen, Entzug des Zugangs, sofern Aufgabe erfüllt ist, Umgang mit den erstellten Daten, Protokollierung der Zugriffe und Dokumentation der Zugänge)		
10	**Werden die Administrativen Zugänge regelmäßig auf deren Notwendigkeit überprüft?** (Vergabe nach Beantragung, Überwachung der zeitlichen Einschränkung, Dokumentation)		
11	**Ist eine Richtlinie für den Umgang mit mobilen Endgeräten vorhanden? Sind die Daten auf diesen geschützt? Weiß der Nutzer mobiler Endgeräte, wie er sich bei Verlust oder Diebstahl verhalten muss?** (Informationen über die auf den Endgeräten erhobenen, verarbeiteten, übertragenen Daten, Verantwortung für die Datensicherung, Risiken und entsprechende Schutzmaßnahmen, Art und Umfang der Software auf den Geräten, Umgang mit diesen , Bedingungen für die Ortung durch die Administration, Verhinderung des unberechtigten Zugriffs z.B. bei Verlust)		
12	**Dürfen Informationen auf mobilen Datenträgern gespeichert und / oder weitergegeben werden? Sind diese durch Verschlüsselung geschützt?**		
13	**Werden die Nutzer über die spezifischen Risiken mobiler Datenträger informiert und sensibilisiert? Ist es untersagt, mobile Datenträger an unberechtigte weiterzugeben bzw. von diesen zu nutzen?** (Viren, Trojaner, Definition eines Verfahrens zur Minimierung des Risikos, Maßnahmen zur Unterbindung unkontrollierter Nutzung)		
14	**Ist der Zugriff auf das Internet durch Schutzmaßnahmen abgesichert?** (Einsatz von aktiven Firewalls und regelmäßige Analyse des Netzwerkverkehrs sowie justieren der Firewall-Regeln zur Erhöhung der Zugriffsschutzes auf das Unternehmensnetzwerk, Protokollierung und Dokumentation der Maßnahmen)		
15	**Erfolgt der Zugriff auf die interne IT-Umgebung über öffentliche bzw. Drahtlose Netze ausschließlich verschlüsselt?** (Verwendung von durch das BSI als sicher definierte Verschlüsselungs-technologien, Festlegung und Dokumentation der Schlüssellänge sowie Protokollierung des Netzwerkverkehrs, Nutzung von sicheren VPN-Tunneln und SSL-Verbindungen)		
16	**Werden regelmäßig Risikoanalysen durchgeführt?** (Auswertung der Protokolle der Firewall, Vorgehensweise nach BSI-Standard 200-3, Identifizieren und Bewerten von Risiken, Bewertung von Schäden, Erkennen von Schwachstellen und definieren von Maßnahmen zur Risikobehandlung)		
17	**Sind die im Einsatz befindlichen IT-Systeme dokumentiert und wird die Aufstellung ständig aktualisiert?** (Aufbau des Unternehmensnetzwerkes, Inventarisierung zur schnellen Lokalisierung, Definition / Beschreibung des Einsatzzweckes – Systemdokumentation)		

Nr.	Frage	JA	NEIN
18	**Existiert ein IT-Sicherheitskonzept?** (regelmäßige Updates, implementierte Testverfahren vor Übernahme in Regelbetrieb, Beschränkung des Netzwerkverkehrs entsprechend der Aufgabenanforderung, Sicherung des Zutritts zu IT-Systemen, Netztrennung z.B. Server mit Storage, Drucker, Arbeitsplätze, Sonderanwendungen, um im Störungsfall den Schaden einzugrenzen, regelmäßige Risikobewertungen- z.B. Abschluss von Versicherungen)		
19	**Ist der Begriff „IT-Sicherheitsvorfall“ eindeutig definiert und eine Richtlinie festgelegt?** (Definition der tolerierbaren Ausfallzeit, Bewertung des Vorfälle, Angemessene Reaktion zur Schadenseindämmung, Meldeketten definieren Situationserfassung, Maßnahmen zum Schutz von Leib und Leben, Schadensdokumentation, Beweismittelsicherung, Schadensbehebung und Nachbereitung)		
20	**Ist ein Notfallplan erstellt und den Mitarbeitern bekannt?** (Wer muss wann was zur Schadenseindämmung und zur Wiederinbetriebnahme ergreifen, an wen ist zu melden? wie sind wann welche Systeme in Betrieb zu nehmen- Wiederanlaufplan, die Pläne sind für jeden und jederzeit im Notfall verfügbar)		
21	**Sind die zentralen IT-Systeme vor physischem Zugriff gesichert? (Zutritt-Schutz)** (Sicherung und Überwachung von Gebäuden, Räumen, Anlagen, Zutritts- und Einbruchssicherheit)		
22	**Sind die zentralen Einheiten vor Brand-, Überspannungs-, Wasser- und Feuerschäden gesichert?** (Feuer-/Rauchmelder, Nutzung der Überwachungsmöglichkeiten in den Servern, Klimaanlagen, Orientierung an VdS 2007, VdS 2010, VdS 2031, VdS 2025, keine direkten Wasserführenden Leitungen in unmittelbarer Nähe, Einsatz von Unterbrechungsfreien Stromversorgungen-USV, Elektrik nach aktuellem Errichter-Standard, Blitzschutz / Gebäudeerdung, Versicherungen)		
23	**Existiert ein Datensicherungskonzept?** (z.B. nach BSI 200-2, Sicherung auf Datenträger, außerhalb des Servers sowie regelmäßige Auslagerung in einen anderen Brandabschnitt, Maßnahmen richten sich nach der jeweiligen Anforderung der Aktualität des Unternehmens, diese Anforderung muss zunächst eindeutig definiert werden die Sicherung und Wiederherstellung muss regelmäßig geprüft werden)		
24	**Werden Dateien nach extern verlagert (Outsourcing)?** (existieren entsprechende Verträge, Vereinbarungen unter Berücksichtigung der aktuellen Rechtslage, des Datenschutzes sowie im Interesse des Unternehmens, Regelungen zur Sicherheit, Dokumentation, Protokollierung der Zugänge, regelmäßige Berichterstattung des Dienstleisters an den Auftraggeber)		
25	**Werden nach Ende des Nutzungszeitraums die Daten auf den Datenträgern unwiederbringlich gelöscht/zerstört?**		
26	**Werden geschäftsrelevante Daten / Kommunikationsdaten rechtssicher behandelt?** (nach GoBD, Geschäftsgeheimnis Gesetz, DSGVO usw.)		
27	**Erfolgt die Ablage bzw. Vernichtung von Geschäftsbriefen/-aufzeichnungen so, dass diese für Unberechtigte nicht einsehbar/nutzbar sind?**		
28	**Existieren mit Ihren Dienstleistern Vereinbarungen, die den Zugriff auf Daten Ihres Unternehmens-Netzwerkes regeln?**		

Versuchen Sie, objektiv diese Fragen zu beantworten!

Auf Basis dieser Antworten kann der aktuelle Stand der Informationssicherheit in Ihrem Unternehmen ermittelt werden, woraus sich weiterführend technische und organisatorische Maßnahmen zur Errichtung des Grundschutzes bzw. zur Erhöhung des Sicherheitsniveaus ableiten lassen.

Wenn es um die IT-Sicherheit Ihres Unternehmens geht, stehen wir Ihnen als kompetenter Partner zur Verfügung:

COMMPACT GmbH
Gesellschaft für Informationstechnologie
COMMPACT GmbH
Gesellschaft für Informationstechnologie
Adolph-Kolping-Str. 6
17034 Neubrandenburg
www.commpact.de
@-Mail: info@commpact.de
Tel.: 0395 56 86 0
Fax: 0395 56 86 150