Erläuterungen zum Ausfüllen des Fragebogens

Generelles

Wir möchten die Sicherheit Ihres Unternehmens erhöhen.

Um das Sicherheitsniveau Ihres Unternehmens zu erkennen, ist die komplette Beantwortung der vorliegenden Fragen notwendig. Im Anschluss hieran erhalten Sie sowohl ein Protokoll der Durchführung als auch einen kompletten Maßnahmenkatalog über sinnvoll vorzunehmende Veränderungen an Ihrer Cyber-Sicherheitseinstellung. Darüber hinaus erhalten Sie auch eine Bewertung Ihres Unternehmens in Bezug auf den aktuellen Cyber-Sicherheitszustand mittels eines vergleichbaren Cyber-Index, auf der Basis der durchgeführten BSI-Umfrage von 2018 und den vorliegenden Antworten aus diesen Fragen.

Der Ihnen vorliegende Fragebogen ist aus Gründen der Übersichtlichkeit in verschiedene Bereiche eingeteilt. Der Aufruf der Erläuterungen erfolgt innerhalb der Fragen und verweist direkt auf die aktuelle Erläuterung der gerade in Arbeit befindlichen Frage. Sie gelangen hiernach sehr einfach wieder zu den Fragen über den Browser-Tab zurück oder Sie können die Erläuterungen auch als ein separates Fenster neben den Fragen positionieren.

Der Begriff **Unternehmen** steht stellvertretend für Firma, Institution, Verein oder öffentliche Verwaltung. Die Fragen beziehen sich auf das Unternehmen des aktuellen Standorts und nicht auf den Konzern, soweit dieser über mehrere Standorte verfügt.

Viele Fragen beinhalten die Antwortmöglichkeiten „**In Planung**“ und „**Später**“, dabei soll „In Planung“ als eine in kurzer Zeit (ca. 3 Monate) durchzuführende Aktion verstanden werden, wobei hingegen „Später“ ausdrücken soll, dass Sie zwar die angesprochene Aktion planen, diese jedoch nicht in einer kurzfristig absehbaren Zeit vollenden können.

Auf die mögliche Antwort: „Trifft nicht zu“ werden für dieses Thema im anschließenden Maßnahmenkatalog keine Maßnahmen erstellt.

Sollten die vorgegeben Antworten nicht exakt Ihre Situation wiedergeben, so wäre die richtige Antwort diejenige, die Ihrer Situation am nächsten kommt. An dieser Stelle wäre es wichtig zu erwähnen, dass die Antworten Ihrer aktuellen Sicherheitseinstellung entsprechen und nicht positiver dargestellt werden sollen, denn nur so können die erarbeiteten Maßnahmen ihr Ziel erreichen.

Sollten Sie die Fragen nicht selbst beantworten können, so wäre es sinnvoll die jeweilige Fachabteilung einzubeziehen – im Sinne einer wahrheitsgetreuen Darstellung des aktuellen Sicherheitsniveaus.

U. Unternehmensdaten

Die nachfolgenden Fragen sind in der Lage Ihr Unternehmen in Bezug auf die Leistungsfähigkeit und der möglichen Anfälligkeit gegenüber Angriffsvektoren zu charakterisieren. Alle diese Fragen bedingen zumindest eine Antwort und sind deshalb auch als Pflichtfragen zu verstehen.

Kennung der Frage	Erläuterung der Frage
U01 Branche	*In welchem Wirtschaftsfeld ist Ihre Institution überwiegend tätig?*
U02 Mitarbeiter	*Wie viele Mitarbeiter beschäftigt Ihre Institution an diesem Standort?*
U03 Umsatz	*Wie hoch war der etwaige Jahresumsatz Ihres Unternehmens in den letzten 12 Monaten bzw. im letzten Geschäftsjahr?*
U04 Region	*Welchen regionalen Geschäftsfokus bedient Ihr Unternehmen (Kunden / Märkte / Geschäftsbeziehungen)?*
U05 Online	*Wie hoch ist der anteilige Online-Umsatz bezogen auf den Gesamtumsatz?*
U06 Cloud	*Nutzt Ihr Unternehmen Cloud-Speicher bzw. Cloud-Dienste?*
	Cloud-Dienste sind sehr vielfältig nutzbar, so können Speicher im Internet verwendet werden, Applikationen werden mittels on Demand zur Verfügung gestellt, auf Backup- und Restore-Verfahren kann zugegriffen werden und vieles mehr.
U07 Kritis	*Gehört Ihr Unternehmen zu den kritischen Infrastrukturen nach dem IT-Sicherheitsgesetz?*
	Kritische Infrastrukturen (KRITIS) sind Organisationen oder Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden. In Deutschland werden Organisationen und Einrichtungen aus den Bereichen Energieversorgung, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung, Finanz- und Versicherungswesen, Staat und Verwaltung sowie Medien und Kultur zu den Kritischen Infrastrukturen gezählt.

	Weitere Informationen, welche Branchen und Sektoren betroffen sind, finden Sie auf der Webseite des BSI unter https://www.bsi.bund.de/DE/Themen/Industrie_KRITIS/KRITIS/IT-SiG/Neuregelungen_KRITIS/Neuregelungen_KRITIS_node.html
U08 Digitalisierungsgrad	*Wie hoch ist der Anteil der EDV-Arbeitsplätze in Bezug auf die Gesamtanzahl der Mitarbeiter?*
	Jeder Mitarbeiter, der mit der EDV in Berührung kommt, ist aufgrund von u.a. Social Engineering-Methoden ein potentielles Risiko für das Unternehmen.
U09 Produktionsgrad	*Wie hoch ist der Anteil der Mitarbeiter in der Produktion in Bezug auf die Gesamtanzahl der Mitarbeiter?*
	Die Kosten bei einem Stillstand in der Produktion sind in der Regel wesentlich höher als diejenigen in der Verwaltung.

B. Bedrohungsabwehr

Mit diesen Fragen wird eine Einschätzung Ihres Unternehmen zum Abwehrverhalten sicherheitsrelevanter Angriffe vorgenommen. Alle diese Fragen bedingen zumindest eine Antwort und sind deshalb auch als Pflichtfragen zu verstehen.

Kennung der Frage	Erläuterung der Frage
B01 IS-Leitlinie	*Gibt es in Ihrem Unternehmen eine Leitlinie zur Informationssicherheit?*
	Eine Sicherheitsleitlinie gibt vor, wie die Ziele der IT-Sicherheit (Verfügbarkeit, Vertraulichkeit, Integrität und Authentizität) erreicht und umgesetzt werden können. Sie legt Verantwortlichkeiten fest und regelt das Vorgehen bei Verstößen. Sie ist wegweisend und gibt somit die unternehmerische Richtung und Entwicklung für die Sicherheit vor.
B02 Organisationsstruktur	*Sind in Ihrem Unternehmen Rollen, Verantwortlichkeiten und Aktivitäten im Bereich Cyber-Sicherheit klar definiert?*
	Die Verantwortlichkeiten im Unternehmen müssen klar geregelt sein, um die notwendige Sicherheit gewährleisten zu können. Üblicherweise gliedern sich die Verantwortlichkeiten in folgende Gruppierung: Das Topmanagement, der Informationssicherheitsbeauftragte (ISB), das Informationssicherheitsteam, die IT-Verantwortlichen, die Administratoren, Vorgesetzte mit Personalverantwortung, das Personal, Projektverantwortliche, Externes Personal und in Lieferanten. Jedem Verantwortlichen muss klar sein, was seine Aufgaben und Pflichten sind und welche Regeln er befolgen muss, um die Informationssicherheit für das Unternehmen gewährleisten zu können. Gerade in kleineren Unternehmen werden verschiedene Verantwortlichkeiten von ein und denselben Personen ausgefüllt sein. Damit das Zusammenspiel der Komponenten trotzdem funktioniert, ist eine besonders klare Zuordnung wichtig.
B03 Datenschutzbeauftragter	*Gibt es in Ihrem Unternehmen einen Datenschutzbeauftragten?*
	Jedes Unternehmen, welches mit personenbezogenen Daten arbeitet, muss die rechtlichen Rahmenbedingungen v.a. der Datenschutzgrundverordnung als auch die des Bundesdatenschutzgesetzes einhalten. In der Regel benötigen Sie hierfür einen DSB, kleinere Unternehmen müssen jedoch keinen DSB benennen dennoch muss der Datenschutz gewährleistet sein. Der DSB muss die Fachkunde und die Zuverlässigkeit besitzen, die Datenschutz-Konformität herstellen bzw. beibehalten zu können. Eine Nichtbestellung führt nicht nur zu Sanktionen, sondern kann auch zu einer in der Öffentlichkeit inakzeptablen Unternehmensführung angesehen werden.

		Dabei sind die wichtigsten Pflichtaufgaben des DSB: - Beratung und Information der Unternehmensführung - Kontrolle der Datenschutz-Strukturen - Übernahme der Zusammenarbeit mit der Aufsichtsbehörde - Anlaufstelle für betroffene Personen
B04	**IT-Sicherheits-beauftragter**	*Gibt es in Ihrem Unternehmen einen IT-Sicherheitsbeauftragten, der ausreichend geschult ist und zeitnahe auf Bedrohungen reagieren kann?*
		Der IT-Sicherheitsbeauftragte ist ein wesentliches Bindeglied in der Kette der Kontrollinstanzen. So handelt er nach dem Sicherheitskonzept bei der Prävention von möglichen Gefährdungen, erkennt und handelt bei Risiken und ist gleichzeitig für die Erstellung, Pflege und Überwachung der Einhaltung des unternehmerischen Sicherheitskonzeptes verantwortlich.
B05	**Datenschutzhand-buch**	*Liegt in Ihrem Unternehmen ein Datenschutzhandbuch vor?*
		Das Datenschutzhandbuch ist eine Sammlung der wichtigsten Dokumentationen, Kommunikations-Protokolle und Nachweisen und dient nicht nur der Einsichtnahme durch die Mitarbeiter und der der Geschäftsführung, sondern auch als Nachweis der Rechenschaftspflicht gegenüber der Aufsichtsbehörde.
B06	**Datenschutzleitlinie**	*Gibt es in Ihrem Unternehmen eine Leitlinie zum Datenschutz?*
		Eine Datenschutzleitlinie, die Grundlage für ein DSMS (Datenschutzmanagement-System), gibt vor, wie die Ziele des Datenschutzes (Verfügbarkeit, Vertraulichkeit, Integrität, Authentizität, Aktualität, Richtigkeit, Rechtssicherheit, Transparenz und Zweckbindung) erreicht und umgesetzt werden können. Sie legt Verantwortlichkeiten, den Zweck für strategische Entscheidungen, die angestrebten Ziele, Anforderungen und Anwendungsbereiche fest und regelt das Vorgehen bei Verstößen. Sie ist wegweisend und gibt somit die unternehmerische Richtung und Entwicklung für den Datenschutz vor.
B07	**Richtlinien**	*Sind Sicherheitsrichtlinien und -verfahren aufgestellt und werden diese beachtet?*
		Eine Richtlinie orientiert sich im Wesentlichen an den Zielvorgaben der jeweiligen Leitlinie und gestaltet diese detailliert aus. Es ist daher empfehlenswert, unterschiedliche Sicherheitsrichtlinien und Teilkonzepte zu erstellen, die einzelne IT-Sicherheitsthemen bedarfsgerecht darstellen. So erhalten Mitarbeiter genau die Informationen, die sie zu einem bestimmten Thema wirklich benötigen, wie z.B. nachfolgende Richtlinien-Vorschläge: - Nutzung der IT - Einsatz und Gestaltung von Passwörtern - Lieferanten und Auftragnehmer

	- IT-Outsourcing Vorhaben - Cloud-Computing - Mobile IT-Systeme - Mobile Datenträger - Datensicherung - Firewall - Entsorgung - Ein- und Austritt von Mitarbeitern - Störungen und Ausfälle - Sicherheitsvorfälle und Wiederanläufe
B08 Vertraulichkeit	*Haben alle Mitarbeiter und Partner eine Vertraulichkeitserklärung unterschrieben?*
	Es sollte eine Vertraulichkeitserklärung unterzeichnet werden, die auch jene Pflichten in Bezug auf Informationssicherheit definiert, die nach Beendigung oder Veränderung des Arbeitsverhältnisses andauern.
B09 Dokumentationen	*Welche Dokumentationen sind erstellt und liegen vor?*
	Die generelle IT-Dokumentation kann dem Tatbestand des fahrlässigen Umgangs mit Informationstechnik entscheidend entgegenwirken. Ein anderer nicht zu vernachlässigender Gesichtspunkt für ausführliche Dokumentationen ist die Abhängigkeit des Unternehmens von Knowhow-Trägern, wodurch die Möglichkeit Informationen zu sichern, gegeben ist.
B10 Schulung	*Wird das Personal in Bezug auf die IT-Sicherheit regelmäßig und umfassend geschult und die Durchführung dieser Schulungen dokumentiert?*
	Es sollte ein Verfahren implementiert sein, das folgende Punkte sicherstellt: 1. Das betroffene Personal wird zielgruppenorientiert über Gefährdungen aufgeklärt und im Umgang mit den vorhandenen Sicherheitsmaßnahmen geschult. 2. Die Inhalte der IS-Leitlinie und sämtlicher relevanter IS-Richtlinien werden vermittelt. 3. Es informiert über Konsequenzen bei Zuwiderhandlung gegen verbindliche Vorgaben. Schulungs- und Sensibilisierungsmaßnahmen sollten mit einem Wissenstest abschließen, um das Verständnis des Personals zu ermitteln und gleichzeitig einen Nachweis der Teilnahme zu erhalten.
B11 Zugriffssicherung	*Sind die wichtigen IT-Systeme, wie z.B. Server und Netzwerkverteiler, vor physischem Zugriff gesichert?*
	Umfangreiche Informationen zum Schutz von Geschäften und Betrieben vor Einbruchdiebstahl haben der GDV (Gesamtverband der deutschen Versicherungswirtschaft) und die VdS Schadenverhütung (ein Unternehmen des GDV) als herstellerunabhängiges Institut in den „Siche-

	rungsrichtlinien für Geschäfte und Betriebe“, VdS 2333, formuliert. Hier werden grundsätzliche Einbruchdiebstahlrisiken und wirksame Gegenmaßnahmen beschrieben. Für die Sicherung von Außengeländen bietet der „Sicherungsleitfaden Perimeter“ VdS 3143, wertvolle Hinweise. IT-Anlagen können auf Grund der gespeicherten Informationen oder des materiellen Wertes der installierten Einrichtungen und Geräte immer wieder Ziel von Einbrüchen und Diebstählen sein. Physische Angriffe auf IT-Anlagen können sowohl von außen als auch von innen erfolgen. Gemäß des „Betriebsartenverzeichnis“, VdS 2559, ist für IT-Anlagen/ Rechenzentren eine Absicherung nach Sicherungsklasse SG 4 vorgesehen. Diese definiert ein sinnvolles Maß an mechanischer Absicherung u. a. von Fenstern und Türen. Für die elektronische Überwachung wird eine Einbruchmeldeanlage der VdS-Klasse C empfohlen, aufgeschaltet auf eine VdS-anerkannte Notruf-Service-Leitstelle. Unter Zuhilfenahme der VdS-Richtlinien und Empfehlungen lassen sich für alle individuellen Risiken und Gewerkkonstellationen angemessene und praxisgerechte Sicherungslösungen erarbeiten. Umfangreiche Informationen zu den VdS-Richtlinien finden Sie unter www.vds.de/richtliniennavigator Quelle: VdS 2007 Informationstechnologie (IT-Anlagen) - Empfehlungen zur Schadenverhütung und zum sicheren Betrieb.
B12 Wiederherstellung	*Können Sie nach Cyber-Sicherheits-Vorfällen Ihre Systeme schnell und effizient wiederherstellen?*
	Kein Unternehmen ist in der Lage, eine längere Zeit ohne funktionierende EDV auszukommen. Die schnelle Wiederherstellbarkeit von Systemen bedingt eine Prüfung der Verwendbarkeit von bereits durchgeführten Sicherungen, und zwar im Vorfeld.
B13 Notfallhandbuch	*Liegt in Ihrem Unternehmen ein Notfallhandbuch vor?*
	Bei einem eingetretenen Notfall stehen in der Regel dafür weder die Zeit noch die Ressourcen zur Verfügung, kurzfristig ein optimales Vorgehen für den Wiederanlauf zielführend einzuleiten. Kopfloses Vorgehen bereitet oftmals einen noch größeren Schaden. Deshalb ist es notwendig, Vorkehrung für das mögliche Schadensereignis zu treffen und die Ausgestaltung eines entsprechenden Regelwerkes vorzunehmen. Diese Dokumentation, die sich nicht nur auf die IT beziehen muss, sollte jedem Mitarbeiter kenntlich gemacht und an einem sicheren und zugleich zugänglichen Ort aufbewahrt werden.
B14 Inventarisierung	*Liegt in Ihrem Unternehmen ein aktueller Inventarisierungsstand vor?*
	Eine aktuelle Inventarisierung ist für das generelle Managen der IT-Infrastruktur unumgänglich. Diese soll nicht nur aufzeigen, welche Geräte derzeitig verfügbar sind, sondern auch Aufschluss geben über Seriennummer, Softwareversion, MAC-Adresse, Anschaffungsdatum,

	Garantiedauer, Lieferanten und bei Software auch über die Lizenzanzahl und deren Bedingungen.
B15 Adminzugang	*Werden administrative Zugänge nur von Administratoren benutzt und diese regelmäßig auf ihre Notwendigkeit überprüft?*
	Es sollten Verfahren für das Anlegen und Ändern von Zugängen und Zugriffsrechte sowie für das Zurücksetzen von Authentifizierungsmerkmalen implementiert werden, die folgende Punkte sicherstellen: 1. Die jeweiligen Vorgänge werden vor ihrer Umsetzung beantragt, geprüft und genehmigt. 2. Zugänge und Zugriffsrechte werden nur genehmigt, wenn sie für die Aufgabenerfüllung des jeweiligen Nutzers oder für die betrieblichen Abläufe des Unternehmens notwendig sind. 3. Wenn ein Nutzer administrative Zugänge oder Zugriffsrechte erhalten soll, wird dies besonders begründet und vom IT-Verantwortlichen entschieden. 4. Antragssteller und Nutzer werden zeitnah über die erfolgte Durchführung informiert; wenn Zugänge entzogen werden, muss nur der Antragssteller informiert werden. 5. Vor dem Löschen eines Zugangs werden die Daten, die mit ihm verknüpft sind, weitergegeben, gelöscht oder gesichert bzw. archiviert. 6. Die jeweiligen Vorgänge werden dokumentiert. Alle Zugänge zu kritischen IT-Systemen sowie sämtliche Zugriffsrechte auf kritische Informationen sollten jährlich erfasst und daraufhin überprüft werden, ob sie benötigt werden. Nicht ordnungsgemäß angelegte Zugänge und Zugriffsrechte sollten als Sicherheitsvorfall behandelt werden.
B16 Adminsegmentierung	*Sind administrative Zugänge nach Zuständigkeit segmentiert und können nur von den dafür vorgesehenen Administratoren benutzt werden?*
	Die Trennung von Zuständigkeiten und entsprechende Delegierung minimiert den Schaden bei eventueller Kompromittierung eines Administrativen Zuganges enorm. Z.B. sollte ein Standortadministrator keine Schreibrechte in der gesamten Verzeichnisstruktur eines Unternehmens haben, sondern nur für seinen Bereich.
B17 Fernzugriff	*Werden administrative Fernzugriffe externer Dienstleister regelmäßig auf ihre Notwendigkeit überprüft?*
	Oftmals werden nach der Beendigung von Geschäftsverhältnissen (z.B. Wechsel der Dienstleister) die Fernzugriffsmethoden nicht deinstalliert bzw. Zugänge auf Systeme unterbunden. Dies sollte in kurzen Zeitabständen geprüft werden.
B18 Zugriffsschutz	*Sind die Daten auf den mobilen Geräten vor unberechtigtem Zugriff geschützt?*

	Die auf dem mobilen IT-System gespeicherten Informationen des Unternehmens sollten vor dem Verlust ihrer Vertraulichkeit und Integrität geschützt werden. Der Schutz der Vertraulichkeit kann z. B. durch eine Verschlüsselung der Datenträger erreicht werden.
B19 Kritische Systeme	*Sind die kritischen IT-Ressourcen und IT-Systeme Ihres Unternehmens bekannt?*
	Die Höhe des möglichen Schadens, der bei einem Störfall auftreten kann, bestimmet, ob eine IT-Infrastruktur als kritisch eingestuft werden soll. Es sollten in definierten Zeitabständen Risikoanalysen der IT-Ressourcen und Systeme durchgeführt werden. Wichtig dabei ist die Klassifizierung von kritischen IT-Ressourcen und Systemen, ohne die ein Geschäftsausfall am wahrscheinlichsten ist.
B20 Kritischer Umgang	*Wie wird mit kritischen IT-Ressourcen bzw. IT-Systemen umgegangen?*
	Kritische IT-Ressourcen müssen anders behandelt werden als nicht kritische, z.B. durch zusätzliche Sicherung, zusätzliche Absicherung oder Schaffen von Redundanzen (Verfügbarkeit bzw. Hochverfügbarkeit durch Cluster). Dafür besteht die Notwendigkeit der Erkennung und der der Differenzierung zwischen kritischen und nicht kritischen Systemen.
B21 Schnittstellen	*Werden externe Schnittstellen, die für Geschäftsprozesse nicht benötigt werden, ausgebaut, stillgelegt, deaktiviert oder anderweitig für Nutzer unzugänglich gemacht?*
	Nicht relevante aber vorhandene Schnittstellen können ein enormes Infektions-/ Angriffsrisiko darstellen. Freie USB-Schnittstellen können genutzt werden, um das System zu infizieren oder Daten unberechtigt zu kopieren und zu entwenden.
B22 Patchmanagement	*Nach welchen Regeln / Verfahren werden Updates eingespielt?*
	„Häufig werden Fehler in Produkten bekannt, die dazu führen können, dass die Informationssicherheit des Informationsverbundes, wo diese betrieben werden, beeinträchtigt wird. Entsprechende Fehler können Hardware, Firmware, Betriebssysteme und Anwendungen betreffen. Diese Schwachstellen müssen so schnell wie möglich behoben werden, damit sie nicht durch interne oder externe Angreifer ausgenutzt werden können. Dies ist ganz besonders wichtig, wenn die betreffenden Systeme mit dem Internet verbunden sind. Die Hersteller von Betriebssystem- oder Software-Komponenten veröffentlichen in der Regel Patches oder Updates, die auf dem jeweiligen IT -System installiert werden müssen, um den oder die Fehler zu beheben. …“, BSI IT-Grundschutz, https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02273.html
B23 Monitoring	*Ist ein Überwachungs- bzw. Monitoring-System für IT-Systeme installiert?*

	Ein reibungsloser Betrieb bedingt die Überwachung bestimmter Komponenten, deren Parameter sich in vorgegebenen Bereichen bewegen dürfen, woraus sich die Ursachen für das mögliche Fehlverhalten ermitteln lassen. Diese Überwachung umfasst inzwischen alle Bereiche der IT, inklusive Sicherheit und Verfügbarkeit.
B24 Netzsicherheit	*Erfolgt ein ausschließlich verschlüsselter Zugriff auf die interne IT-Infrastruktur über öffentliche (z.B. VPN) oder drahtlose Netze?*
	Drahtlose Netzwerke und die Anbindung an öffentliche Netze sollten ausreichend geschützt werden. Zur Verschlüsselung von drahtlosen Netzwerken sollte mindestens WiFi Protected Access 2 (kurz WPA2) genutzt werden (WPA3 wird derzeitig als neuer Standard vorbereitet). WPA2 implementiert die grundlegenden Funktionen des Sicherheitsstandards IEEE 802.11i, in dessen Zusammenhang auch der Begriff Robust Security Network (RSN) verwendet wird. Die Anbindung über öffentliche Netze sollte über eine verschlüsselte Verbindung mindestens mit Hilfe der Technologien VPN und SSL hergestellt werden.
B25 Backup	*Wie handhabt Ihr Unternehmen den Umgang mit Backups?*
	Daten können unbrauchbar werden oder verloren gehen. Deshalb ist es notwendig, durch eine Datensicherung die Integrität und Verfügbarkeit der Daten sicherzustellen. Die Datensicherung kann auf Basis eines anerkannten Standards wie z. B. BSI-Standard 200-2 unter Berücksichtigung der IT-Grundschutz-Kataloge des BSI implementiert werden. Sicherungs- und Wiederherstellungsverfahren sollten mindestens folgendermaßen getestet werden: 1. Einmal jährlich wird ein gesichertes IT-System nach dem Zufallsprinzip ausgewählt und in einer Testumgebung wiederhergestellt. 2. Nach jeder Änderung des Sicherungs- oder des Wiederherstellungsverfahrens wird eines der betroffenen IT-Systeme gesichert und in einer Testumgebung wiederhergestellt. Die Tests sollten ohne Unterstützung durch den jeweiligen Verantwortlichen für die Datensicherung erfolgen. Vielmehr sollten sie von einem anderen Mitarbeiter anhand der vorliegenden Dokumentation bewältigt werden können. Die vorhandenen Sicherungs- und Wiederherstellungsverfahren sollten anhand der Ergebnisse und Erkenntnisse der Tests zeitnah überarbeitet werden. Die Durchführung und die Ergebnisse der Tests sind zu dokumentieren. Für die Datensicherung, -wiederherstellung und -archivierung sollten Verfahren implementiert werden, die folgende Punkte sicherstellen: 1. Die gesicherten Daten werden bei Übertragung, Lagerung und Transport vor Änderungen, Beschädigung, Verlust und unberechtigter Einsichtnahme geschützt. 2. Die gesicherten Daten werden nicht im gleichen Brandabschnitt wie die gesicherten IT-Systeme aufbewahrt. Einzelne Datensicherungen

		sollten an einem entfernten Standort aufbewahrt werden, damit die Datensicherung auch im Katastrophenfall verfügbar bleibt.
B26	**Log-Dateien**	*Werten Sie Log-Daten zur Erkennung von Cyber-Angriffen aus?*
		Log-Dateien können Aufschluss über den IT-Sicherheitsstatus Ihres Unternehmens geben. So können die Auswertungen solcher Informationen einen umfangreichen Überblick über Probleme und Sicherheitsvorfälle liefern. Gesetzliche Vorschriften wie ISO-27xxx-Regularien, SOX, HIPAA oder PCI-DSS-Standards zwingen Unternehmen Informationen über ihren Netzwerkverkehr zu archivieren, um diesen auch später noch analysieren zu können. Weitere Gesetze wie die DSGVO / BDSG und auch das IT-Sicherheitsgesetz verpflichten Unternehmen zur direkten Auswertung und zum Handeln, um ihre IT-Systeme vor Cyberangriffen zu schützen. SIEM-Lösungen können diese Unternehmen vor allem in dem Punkt der strukturierten und transparenten und vor allem sicheren Aufbewahrung von Daten unterstützen.
B27	**Produktionsnetz-zugang**	*Wird der direkte Online-Zugang, bzw. Online-Zugriff auf das Produktionsnetzwerk verhindert?*
		Das Produktionsnetzwerk ist in der Regel mit veralteten Betriebssystemen ausgestattet, die gegenüber einem aktuellen Verwaltungsnetz eine überproportionale Anzahl an Schwachstellen aufweist, insofern ergibt sich ein wesentlich erhöhtes Schadensrisiko, wenn ein Onlinezugriff vorhanden ist. Der Schutz eines Produktionsnetzwerkes muss höher bewertet werden als das einer Verwaltung. Auch sollte die Übertragung zwischen Produktionsstätten klar definiert sein und über die richtigen Regeln in den Firewalls gelöst werden.
B28	**Produktionsnetz-trennung**	*Ist das Produktionsnetzwerk vom Verwaltungsnetzwerk getrennt?*
		Die Abschottung des Produktions- vom Verwaltungs-Netzwerk ist eine Grundanforderung (siehe IEC 62443-3-2). Optional kann eine weitere Unterteilung in Zonen erfolgen. Der sorgfältigen und restriktiven Festlegung der Firewall-Regeln kommt in diesem Zusammenhang eine hohe Bedeutung zu. Zu einer Defense-in-Depth-Strategie kann auch die Nutzung virtueller Netzwerke (VLAN) gehören, um unterschiedliche Zonen in der Anlage zu bilden.
B29	**Schadsoftware**	*Verfügt jedes IT-System über einen dem Stand der Technik angepassten Schutz vor Schadsoftware (Echtzeitschutz, Verhaltensüberprüfung), erfolgt eine tägliche vollständige Untersuchung auf Anwesenheit von Schadsoftware und wird regelmäßig aktualisiert?*
		„Jede Institution sollte geeignete vorbeugende Maßnahmen gegen Schadprogramme zusammenstellen sowie das Vorgehen im Fall einer

	Infektion mit Schadprogrammen regeln. Unter Schadprogrammen werden neben den klassischen Computer-Viren auch Trojanische Pferde, Computer-Würmer und weitere Schaden verursachende Software verstanden. Als Grundlage, um das Eindringen von Schadprogrammen in IT-Systeme zu verhindern, sollte ein Sicherheitskonzept gegen Schadprogramme entwickelt werden…“, BSI IT-Grundschutz B 1.6, https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/baust/b01/b01006.html
B30 Archivierung	*Erfolgt eine gesetzeskonforme Archivierung von Dokumenten, Dateien und Emails?*
	Die gesetzlichen Erfordernisse erwarten den Einsatz einer Archivierungslösung für alle elektronischen Dokumente für Unternehmen, die Geschäfte auf dem digitalen Weg abwickeln (GoBD).
B31 Penetrationstest	*Werden Penetrationstests zum Aufspüren von Schwachstellen durchgeführt?*
	Pentests sind in der Regel umfassende Tests an Netzwerken zur Prüfung der Sicherheit von IT-Systemen mit Mitteln und Methoden, die ein Angreifer verwenden würde, um ein System zu kompromittieren. Pentests sind in der Lage den aktuellen Sicherheitsstand aus der Sicht eines Angreifers zu bestimmen, um so die aufgezeigten Schwachstellen schließen zu können. Im Sinne einer steten Verbesserung der Unternehmenssicherheit sollen diese Tests kontinuierlich durchgeführt werden.
B32 Meldung	*Gibt es in Ihrem Unternehmen eine Richtlinie für die Meldung von außergewöhnlichen Ereignissen?*
	Außergewöhnliche Ereignisse sind Störungen im Verfahrensablauf. Diese Störungen sind zu erkennen und in Datenpanne bzw. Sicherheitsvorfall einzuordnen. Je nach Störungsart sind entsprechende Meldungen durchzuführen - Interne Meldungen an den jeweiligen Vorgesetzten, Verantwortlichen - Meldung an die Datenschutzaufsichtsbehörde - Benachrichtigung aller betroffenen Personen oder Aufgabe einer überregionalen Anzeige für die betroffenen Personen.
B33 Cloud Computing	*Werden für jede Nutzung von Cloud-Computing Anforderungen an die Sicherheit definiert?*
	Bei der Entscheidung für Cloud-Computing ist man nicht mehr Herr seiner Daten. Wo sie sich auch immer befinden, im oder auch außerhalb des Euroraumes, die Sicherheit bedingt ein erhöhtes Augenmerk.
B34 IT-Outsourcing	*Werden für jedes IT-Outsourcing Vorhaben Anforderungen an die Sicherheit definiert?*

	Die Vertragsgestaltung bei IT-Outsourcing Vorhaben muss sowohl die Sicherheit der Datenverarbeitung als auch die Einflussnahme auf Umfang und Qualität der Dienstleistung berücksichtigen und so gestaltet sein, dass der wesentlichste Nachteil eines Outsourcings, die Knowhow-Übertragung, klar geregelt ist.
B35 Supportende	*Wie werden nicht mehr in der Wartung befindliche IT-Systeme behandelt?*
	Die Wartung von IT-Systemen wir in der Regel durch Patches und Updates vorgenommen. Damit werden bekannte Sicherheitslücken geschlossen. Was aber, wenn diese Wartung z.B. aufgrund des Alters des Systems abgekündigt wird und die bekannten Sicherheitslücken nicht mehr geschlossen werden? Diese Frage muss beantwortet werden, wenn solche Systeme weiter benutzt werden müssen.

C. Cyber-Potential

Diese Rubrik Fragen dient zur Einschätzung der eigenen Sicherheitslage. Alle diese Fragen bedingen zumindest eine Antwort und sind deshalb auch als Pflichtfragen zu verstehen.

Kennung der Frage	Erläuterung
C01 Angriffsziel	*War Ihr Unternehmen schon einmal das Ziel eines erfolgreichen Cyber-Angriffs?*
C02 Gefährdung	*Stellen Cyber-Angriffe eine relevante Gefährdung für die Betriebsfähigkeit Ihres Unternehmens dar?*
C03 Risikobewertung	*Hat sich die Bewertung der Risiken durch Cyber-Angriffe für Ihr Unternehmen in diesem Jahr verändert?*
C04 Angreifergruppen	*Von welcher Cyber-Angreifer-Gruppe erwartet Ihr Unternehmen in den kommenden zwei Jahren die größte Bedrohung?*
C05 Angriffsarten	*Von welcher Cyber-Angriffsart wird in den kommenden zwei Jahren für Ihr Unternehmen die größte Bedrohung ausgehen?*
C06 Schutzmaßnahmen	*Welche Maßnahmen sollten in Ihrem Unternehmen zum Schutz gegen Cyber-Angriffe umgesetzt werden, die bislang noch nicht betrachtet worden sind?*
C07 Schutzbedarf	*Sind die in Ihrem Unternehmen getroffenen Maßnahmen zum Schutz gegen Cyber-Angriffe aus Ihrer Sicht ausreichend?*
C08 Fallbeispiel	*Nehmen wir an, ein Mitarbeiter hat versehentlich in Ihrem Unternehmen eine Ransomware-Infektion ausgelöst, die sich nun im eigenen Netzwerk sehr rasch ausgebreitet hat, bevor Sie Gegenmaßnahmen ergreifen konnten.* *Wie wird Ihr Betrieb hierauf reagieren?*

P. Persönliche Daten

Die Rubrik gibt Angaben zum Unternehmen und zur Person. Nur die Fragen mit einem * bedingen eine Antwort und sind deshalb auch als Pflichtfragen zu verstehen, alle anderen Angaben sind als freiwillig zu verstehen.

Kennung der Frage	Erläuterung der Frage
P01 Anrede*	*Anrede:*
P02 Vorname*	*Vorname:*
P03 Nachname*	*Nachname:*
P04 Titel / Funktion	*Titel / Funktion:*
P05 Unternehmen	*Unternehmen:*
P06 Straße / Nr	*Straße / Nr:*
P07 Postleitzahl	*Postleitzahl:*
P08 Stadt	*Stadt:*
P09 Email*	*Email:*
	Die Angabe Ihrer Email-Adresse dient uns zur direkten Kommunikation mit Ihnen.
P10 Webseite	*Haupt-Webseite:*
	Unternehmens-Webseite Ihres Unternehmens
P11 Telefon	*Telefon:*
	Wenn Sie möchten, können Sie hier Ihre Telefonnummer angeben, so

	können wir Sie im Falle von möglichen Unklarheiten kontaktieren, dies wird jedoch in der Regel nicht notwendig werden.
P12 Notiz	*Notiz:*
	An dieser Stelle können Sie uns Bemerkungen, Informelles, Zustimmung, Ablehnung mitteilen. Sagen Sie uns einfach, was Ihnen gefällt oder was Sie stört. Wir freuen uns auf jeden Fall über Ihre Reaktion, die wir gerne berücksichtigen werden.
P13 Kennwort*	*Kennwort:*
	Das von Ihnen vergebene Kennwort wird für die Verschlüsselung der zu versendenden PDF-Dateien benutzt, so kann auch nur derjenige diese PDF-Dateien lesen, der die Fragen beantwortet, bzw. abgeschickt hat.
P14 CR-Agentur	*Cyber-Ranking Agentur:*
	Wir haben in Deutschland ein Netz von Cyber-Ranking Agenturen aufgebaut, die Ihnen bei der Bestimmung Ihres aktuellen Sicherheitsniveaus und weiter bei der Durchführung der vorgeschlagenen Maßnahmen behilflich sind. Die Nennung einer speziellen Kennung der Agentur führt automatisch zur Weitergabe der Daten an diese Agentur. An dieser Stelle können Sie sich jedoch sicher sein, dass alle Maßnahmen unsererseits ergriffen worden sind, Ihre Daten vor weiterer Verbreitung zu schützen (z.B. mittels Verträge, NDA, verschlüsselte Übertragung, spezielle Auswahl und Schulung).