**Unverbindliche Bekanntgabe des Gesamtverbandes der Deutschen Versicherungswirtschaft e.V. (GDV) zur fakultativen Verwendung.
Abweichende Vereinbarungen sind möglich.**

Unverbindlicher Muster-Fragebogen zur Risikoerfassung im Rahmen von Cyber-Versicherungen für kleine und mittelständische Unternehmen

Stand: Dezember 2019

Konzept

Einsatzzweck

Der vorliegende Muster-Fragebogen soll es einem Erstversicherer ermöglichen, das Risiko- und Schadenspotenzial eines Versicherungsnehmers mit wenigen Fragen grob, aber aussagekräftig zu erfassen.

Um die Anzahl der zu stellenden Fragen zu minimieren, besteht der Fragebogen aus mehreren Bereichen, die jeweils nur unter bestimmten Bedingungen erfasst werden. Die Bereiche werden nach Risiko-Kategorien und Geschäftsfeldern unterschieden. Die Musterbedingungen für eine Cyberrisiko-Versicherung und dieser Muster-Fragebogen sind unabhängig voneinander als unverbindliche Muster-Bausteine eines Cyberversicherungskonzepts verwendbar.

Der vorliegende Muster-Fragebogen zielt überwiegend auf den externen Täter ab. Aufgrund des Wirkungskreises und der Tatmöglichkeiten interner Täter geht von diesen jedoch generell eine deutlich höhere Gefahr aus als von externen Tätern: Interne Täter können im Vergleich zu externen Angreifern Sicherheitsvorkehrungen oftmals einfacher und unbemerkt umgehen. So können sich interne Täter unter Umgehung geringerer Hürden physischen Zugang und/oder auch technischen Zugriff auf Daten und Systeme verschaffen. Der Muster-Fragebogen hat für das Risikoszenario des vorsätzlich handelnden Mitarbeiters daher nur eingeschränkte Aussagekraft. Ist in den Versicherungsbedingungen – wie in den unverbindlichen Musterbedingungen – die vorsätzliche Herbeiführung eines IT-Sicherheitsvorfalls durch Mitarbeiter des Versicherungsnehmers vorgesehen, ist dieses Risiko gesondert zu erfassen und zu bewerten.

Risiko-Kategorien

Es werden drei Risiko-Kategorien unterschieden, die sich primär am Jahresumsatz des Versicherungsnehmers orientieren. Grundlage dieser Erwägung ist, dass der Jahresumsatz den allgemein stärksten Indikator für das Schadenspotenzial des Versicherungsnehmers darstellt. Bei geringem Schadenspotenzial soll die Bearbeitung des Fragebogens, damit aber auch der Detailgrad der Erfassung des Schutzniveaus, minimiert werden. Bestimmte Geschäftsbereiche unterliegen unabhängig vom Jahresumsatz des Versicherungsnehmers einem höheren Schadenspotenzial. Dazu gehören:

- der Betrieb von e-Commerce auf eigener Infrastruktur, weil damit der Betrieb eines Zahlungssystems und das Sammeln entsprechender Kundendaten einhergeht,
- die Verarbeitung sensibler Daten, weil damit die Verpflichtungen im Rahmen der Datenschutzgrundverordnung und des Bundesdatenschutzgesetzes einhergehen,
- die Verarbeitung von Berufsgeheimnissen sowie
- die Verarbeitung von Betriebsgeheimnissen Dritter, weil diese einem höheren Angriffsrisiko und einem höheren Drittschadenspotenzial unterliegen,
- der Betrieb von industriellen Kontrollsystemen, weil im Falle eines Angriffs durch Betriebsunterbrechungs- und Reparaturkosten potenziell hohe Schäden drohen.

Sofern eine Tätigkeit in diesen Bereichen vorliegt, erfolgt unabhängig vom Jahresumsatz eine Erhöhung der Risikokategorie. Die vom Versicherungsnehmer zu beantwortenden Fragen umfassen

1. alle Fragen der zugeordneten Risiko-Kategorie
2. falls zutreffend, alle Fragen niedrigerer Risiko-Kategorien
3. falls zutreffend, alle Zusatzfragen zu bestimmten Geschäftsbereichen.

Die Fragen der Risikokategorie A erfassen daher nur die allgemeine Einhaltung der Obliegenheiten. Darüber hinaus werden Tätigkeiten in bestimmten Geschäftsbereichen erfasst, mit denen eine höhere Risikoeinstufung oder eine Erweiterung des Fragenbereichs einher-

gehen. Die Beantwortung ist für alle Versicherungsnehmer obligatorisch. Sie ist ausreichend, sofern der Versicherungsnehmer nicht in den oben genannten Geschäftsbereichen tätig ist und sein Jahresumsatz unter 2 Mio. EUR liegt. Dies ist bei ca. 80 % der kleinen und mittelständischen Unternehmen der Fall.

Für Versicherungsnehmer mit einem Jahresumsatz von bis zu 5 Mio. EUR sind zusätzlich die Fragen der Risiko-Kategorie B relevant. Die Fragen der Risiko-Kategorie C sind bis zu einem Jahresumsatz von 10 Mio. EUR vorgesehen.

Bei Unternehmen mit einem Jahresumsatz von mehr als 10 Mio. EUR ist der vorliegende Muster-Fragebogen ggfs. durch eine darüber hinausgehende individuelle Erfassung des Risikopotenzials zu ergänzen.

Die Kriterien der Risiko-Kategorien A-C sind in Tabelle 1 dargestellt.

Tabelle 1. Kriterien der Risiko-Kategorien A-C.

Risiko-Kategorie	Kriterien
A	▪ Jahresumsatz <= 2 Mio. EUR ▪ *Keiner* der folgenden Geschäftsbereiche: o e-Commerce mit eigener Infrastruktur o Verarbeitung sensibler Daten, insb. personenbezogene Daten Dritter o Berufsgeheimnisse o Betriebsgeheimnisse Dritter o Industrial Control Systems (ICS)
B	▪ Jahresumsatz <= 5 Mio. EUR ▪ *Max. einer* der folgenden Geschäftsbereiche o e-Commerce mit eigener Infrastruktur o Verarbeitung sensibler Daten, insb.: besondere personenbezogene Daten Dritter o Berufsgeheimnisse o Betriebsgeheimnisse Dritter o Industrial Control Systems (ICS)
C	▪ Jahresumsatz <= 10 Mio. EUR

Obliegenheiten

Die Fragen der Risiko-Kategorie A decken bestimmte Basis-Obliegenheiten ab, die auch in den Musterbedingungen für eine Cyberrisiko-Versicherung zu finden sind. Die minimale Anzahl der vom Versicherungsnehmer zu beantwortenden Fragen ist in Abbildung 1 gestellt und beinhaltet 10 Fragen aus dem Bereich der Obliegenheiten sowie 5 weitere Fragen zu Sonderbereichen. Diese Fragen dienen der Erfassung, ob der Sonderbereich im Fragebogen abgedeckt werden muss und ziehen entsprechend potenziell weitere Fragen nach sich.

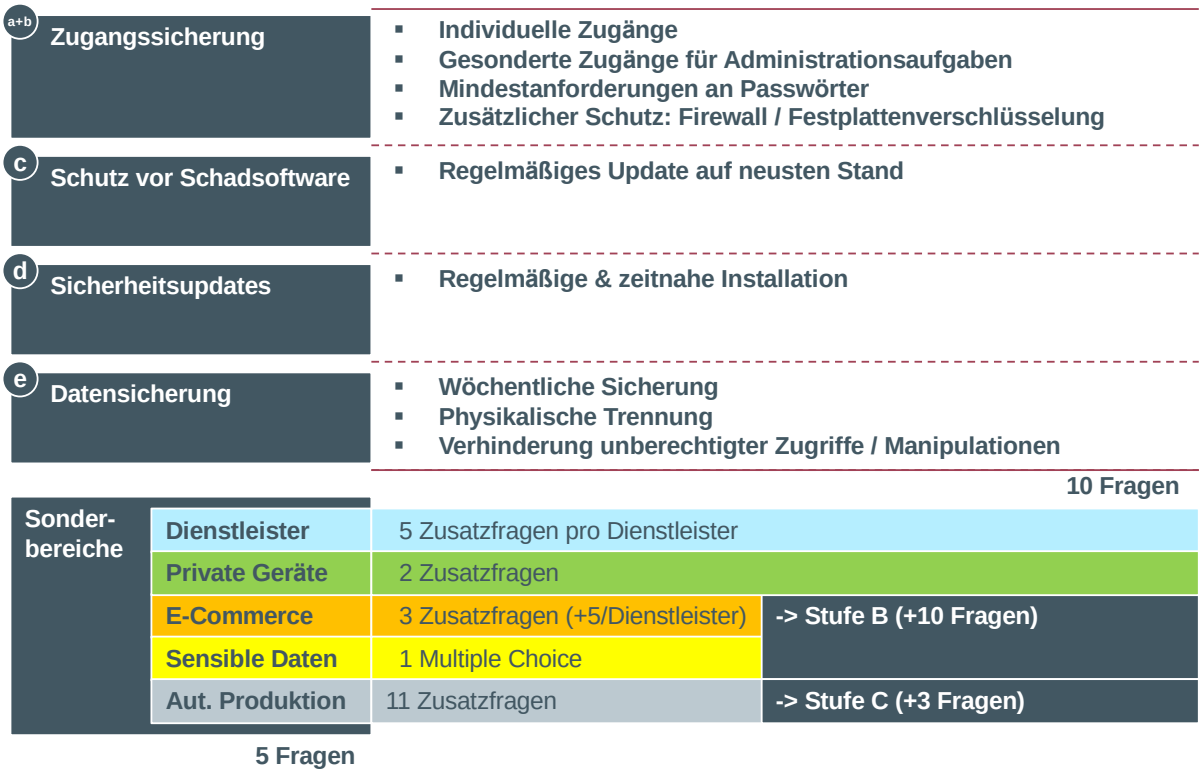

Abbildung 1. Abdeckung der Obliegenheiten und Erfassung der Sonderbereiche.

In den höheren Risiko-Kategorien werden weitere Bereiche der Informationssicherung, insbesondere organisatorische Sicherheit, Netzwerkseparation und der Schutz sensibler Daten erfasst. Weiterhin kommen Fragen zur versicherungstechnischen und rechtlichen Risiko-Einstufung hinzu. Tabelle 2 bietet einen Überblick, welche Themenbereiche in welchen Fragebogenteilen betont werden.

Tabelle 2. Verteilung der Fragen auf Themenbereiche und Risiko-Kategorien.

		A	B	C	Dienst-leister	Private Geräte	E-Com-merce	Sensible Daten	ICS	∑
OBLIEGENHEIT	Zugang / Zugriff	4	3						3	10
	Schutz vor Schadsoftware	1								1
	Patching Sicherheits-updates	1	1						1	3
	Backup Datensicherung	4							2	6
	Organisatorische Sicherheit		3	2					2	7
	Netzwerk-separation		1			1			3	5
	Schutz sensibler Daten			1		1				2
	Risikoeinstufung			1	5		3	3		12
	∑	10	8	4	5	2	3	3	11	

Zusatzfragen: Geschäftsfelder und Besonderheiten

Einige Geschäftsfelder sowie bestimmte Praktiken im Umgang mit Daten oder informationstechnischen Systemen erfordern eine genauere Erhebung, um das Risikopotenzial eines Versicherungsnehmers genau zu erfassen.

Die Bereiche umfassen im Einzelnen:

1. **E-Commerce:** Die Abwicklung von Geschäfts-, insb. Zahlungsvorgängen über Online-Angebote bietet eine attraktive und schadensträchtige Oberfläche für Angriffe.
2. **Dienstleister:** Die Auslagerung zentraler Komponenten der Infrastruktur an Dienstleister unterliegt individuellen vertraglichen Vereinbarungen beider Parteien hinsichtlich Haftung sowohl im Eigen- als auch im Drittschadensbereich. Die Gestaltung dieser Vereinbarungen betrifft direkt das für den Versicherer relevante Schadenspotenzial.
3. **Privatgeräte:** Die Verwendung von privaten Geräten durch Mitarbeiter hat zur Folge, dass diese nicht einem zentralen Sicherheitsmanagement durch den Versicherungsnehmer unterliegen.
4. **Datenschutz:** Die Verarbeitung besonders schützenswerter Daten unterliegt rechtlichen Vorgaben und einer besonderen Sorgfaltspflicht.
5. **ICS:** Automatisierte Produktionsprozesse (auch: *ICS – industrial control systems*) werden im Standardfragebogen nicht erfasst und bedürfen einer gesonderten Erfassung.

Online-Version

Welche Fragen zu beantworten sind, richtet sich nach der Risiko-Kategorie und den Geschäftsfeldern und Besonderheiten der Versicherungsnehmer. Dieser dynamische Prozess lässt sich in Papierform nur wenig ansprechend umsetzen. Es empfiehlt sich eine dynamische Beantwortung in einer Digital- bzw. Online-Version.

Eine solche Online-Version stellt der GDV unter dem Namen Cyber-Sicherheitscheck[1] bereit. Die Online-Version des Fragebogens bietet 5 Vorteile zur Unterstützung des Erstgesprächs:

1. **Nutzerfreundlichkeit:** Zu jeder Frage werden Hintergründe und Unterstützung bei der Beantwortung angeboten. Ein Fortschrittsbalken zeigt die verbleibenden Fragen bis zur (Zwischen-)Auswertung an.
2. **Interaktivität:** Die Nutzer erhalten zu jeder beantworteten Frage ein kompaktes inhaltliches Feedback. Bei Antworten, die auf fehlende Sicherheitsmechanismen hindeuten, werden Empfehlungen und weiterführende Informationen angeboten.
3. **Information:** Die Nutzer können sich über ihren Sicherheitsstand informieren und diesen mit der Referenzpopulation und den *best practices* vergleichen. Nach dem Ausfüllen von Teilabschnitten des Fragebogens erhalten die Nutzer eine grafische Zwischenauswertung zu Einschätzung ihres Schutzniveaus.
4. **Empfehlungen:** Diese Auswertung enthält priorisierte Empfehlungen zur Verbesserung des Schutzniveaus. Bei Bedarf werden nützliche Tipps zur Erhöhung der eigenen IT-Sicherheit gegeben. Dies hilft Versicherungsnehmern dabei, ihre Sicherheitsvorkehrungen sinnvoll zu erhöhen.
5. **Weiterverwendung:** Um ein wiederholtes Beantworten derselben Fragen zu vermeiden, lassen sich die Antworten nach Abschluss des Fragebogens im gängigen Datenaustauschformat JSON herunterladen. Dieses Format ist geeignet zum universellen Datenimport. Darüber hinaus wird die Möglichkeit zum Ausdrucken und Speichern angeboten.

Die Online-Version des Fragebogens stellt der GDV seinen Mitgliedsunternehmen kostenlos zur Integration in eigene Systeme bereit. Darüber hinaus stellt der GDV ebenfalls kostenlos ein Tool zum Datenimport bereit.

Fragen

Um eine effiziente und aussagekräftige Beantwortung der Fragen zu ermöglichen, erfolgt die Beantwortung der Fragen, sofern nicht anders angegeben, in folgendem Format:

- ☐ Ja, trifft zu
- ☐ Nein, nicht zutreffend

Dieses Format vereinfacht ebenfalls die statistische Auswertung und Validierung der Fragen im Hinblick auf die Vorhersage des Versicherungsfalls- und Schadenpotenzials. Im Folgenden werden die Fragen und Ihre Relevanz dargestellt und zwei Formulierungsmöglichkeiten vorgeschlagen. Grundsätzlich empfiehlt der GDV die *vereinfachte Formulierung*.

[1] Online-Fragebogen:
https://www.gdv.de/cybercheck
Siehe auch:
https://www.gdv.de/de/medien/aktuell/cyber-sicherheitscheck-fuer-den-deutschen-mittelstand-42974

Allgemeine Erfassung des Geschäfts- und Risikofeldes

Einige Geschäftsfelder sowie bestimmte Praktiken im Umgang mit Daten oder informationstechnischen Systemen erfordern eine genauere Erhebung, um das Risikopotenzial eines Versicherungsnehmers adäquat zu erfassen.

E1. E-Commerce auf eigener Infrastruktur

Relevanz: Im e-Commerce sind die Kernbereiche des Geschäfts einem direkten Angriffsrisiko ausgesetzt. Durch die Bearbeitung entsprechender Kunden- und Zahlungsdaten bietet sich darüber hinaus ein hohes Drittschadenpotenzial.

Aus diesem Grund sind Versicherungsnehmer mit Tätigkeit im e-Commerce unabhängig vom Jahresumsatz in der Kategorie B anzusiedeln.

Sofern der Versicherungsnehmer den Betrieb selbst unterhält und administriert, sind darüber hinaus die Zusatzfragen E-Commerce zu beantworten. Werden diese Kernaufgaben des Geschäfts an Dritte ausgelagert, sind diese im Rahmen der Zusatzfragen Dienstleister zu erfassen.

Standard-Formulierung: *Wir betreiben eine eigene Infrastruktur für Online-Handel (e-Commerce).*

Vereinfachte Formulierung: *Betreiben Sie einen Online-Shop mit eigenem IT-System?*

E2. Verarbeitung von Daten Dritter

Relevanz: Wenn der Versicherungsnehmer im Bereich der Auftragsdatenverarbeitung tätig ist, muss das Drittschadenpotenzial entsprechend mit den Zusatzfragen Datenverarbeitung erfasst werden. Aufgrund des höheren notwendigen Schutzniveaus ist der Versicherungsnehmer unabhängig vom Jahresumsatz in der Kategorie B anzusiedeln.

Standard-Formulierung: Wir speichern und verarbeiten Daten von Dritten.

Vereinfachte Formulierung: *Speichern Sie Daten von Dritten? (Kunden, Lieferanten, Mitarbeiter, Geschäftspartner etc.)*

E3. Datenverarbeitung durch Dienstleister

Relevanz: Laut Art. 28 Datenschutz-Grundverordnung (DSGVO) ist der Auftraggeber für die Einhaltung der Vorschriften der DSGVO und anderer Vorschriften über den Datenschutz verantwortlich, wenn personenbezogene Daten im Auftrag durch andere Stellen erhoben, verarbeitet oder genutzt werden.

Ziel ist es, den allgemeinen IT-Betrieb zu erfassen. Alltagsdienstleistungen wie E-Mail fallen nicht in den für diese Frage relevanten Bereich. Werden jedoch Kernaufgaben der Datenverarbeitung an Dritte ausgelagert, so sind diese im Rahmen der Zusatzfragen Dienstleister zu erfassen.

Standard-Formulierung: *Wir nutzen einen Dienstleister zur Auftragsdatenverarbeitung nach Art. 28 DSGVO.*

Vereinfachte Formulierung: *Nutzen Sie einen Dienstleister zur Datenverarbeitung (Auftragsdatenverarbeitung nach Art. 28 DSGVO)?*

E4. Nutzung privater Geräte

Relevanz: Mitarbeitereigene Geräte unterliegen nicht der Verwaltung durch den Versicherungsnehmer und können somit auf einem höheren oder niedrigeren als dem vorgegebenen Sicherheitsniveau angesiedelt sein. Aufgrund der fehlenden Erfassung ist von einem niedrigeren Sicherheitsniveau auszugehen, welches weitere Schutzmaßnahmen erfordert, die in den Zusatzfragen Private Geräte erfasst werden.

Standard-Formulierung: *Die Nutzung privater Geräte ist in unserer Unternehmens-IT gestattet.*

Vereinfachte Formulierung: *Dürfen Mitarbeiter private Geräte in Ihrem Unternehmensnetzwerk nutzen?*

E5. Automatisierte Produktionssysteme

Relevanz: Beim Betrieb von automatisierten Produktionssystemen (ICS) drohen im Falle eines Angriffs hohe Schäden durch Betriebsunterbrechung und Reparaturkosten. Aufgrund des hohen Verfügbarkeitsanspruchs werden ICS-Anlagen oft nicht regelmäßig auf den aktuellen Stand gebracht, was ein weiteres Risiko für ihren Betrieb darstellt. Diese erhöhten Risiken können nur durch besondere Maßnahmen abgedeckt werden, die in den Zusatzfragen Vernetzte Produktionssysteme erfasst werden. Sollte der Versicherungsnehmer nicht aufgrund seines Jahresumsatzes in der höchsten Risikokategorie angesiedelt sein, werden dennoch die Schutzmaßnahmen der Kategorie B und Kategorie C notwendig.

Standard-Formulierung: *Wir nutzen automatisierte Produktionssysteme (ICS).*

Vereinfachte Formulierung: *Nutzen Sie automatisierte Produktionssysteme mit Netzanbindung?*

Kategorie A

Die Schutzmaßnahmen für Versicherungsnehmer der Risiko-Kategorie A decken die oben erwähnten Basis-Obliegenheiten ab. Für Versicherungsnehmer mit einem Jahresumsatz unter 2 Mio. EUR, die nicht in einem besonderen Bereich erhöhten Risikos tätig sind, ist der Fragebogen mit Beantwortung dieser Fragen abgeschlossen.

A1. Individuelle Zugänge

Obliegenheit: Zugangssicherung

Relevanz: Systeme ohne Authentifizierung können von Angreifern ohne Hindernis übernommen und kontrolliert werden. Benutzerindividuelle Kennungen sind darüber hinaus notwendig, um die Zugriffsrechte einzelner Accounts granular zu definieren und nachvollziehen zu können, welche angriffs- oder schadensrelevanten Tätigkeiten zu welchem Zeitpunkt von welchem Nutzer durchgeführt wurden. Werden an kritischen Stellen sogenannte „Funktionsaccounts“ genutzt, also Login-Daten, die sich mehrere Personen teilen, kann die Verbreitung der Zugangsdaten nicht sinnvoll kontrolliert oder gestoppt werden.

Standard-Formulierung: *Für jeden Nutzer und Administrator ist eine benutzerindividuelle Kennung/Zugang mit Passwort vergeben. Für den Zugang zu jedem System sind eine Benutzerkennung und ein Passwort notwendig.*

Vereinfachte Formulierung: *Hat jeder Nutzer und Administrator eine eigene, mit einem individuellen Passwort geschützte Zugangskennung für Ihre IT-Systeme?*

A2. Passwortqualität

Obliegenheit: Zugangssicherung

Relevanz: Einfach zu erratende oder an mehreren Stellen wiederverwendete Passwörter sind eines der häufigsten Einfallstore für Angreifer. Aus diesem Grund ist es notwendig, Nutzer daran zu hindern, vorhandene technische Sicherheitsmaßnahmen durch einfache Passwörter zu schwächen.

Standard-Formulierung: *Wir haben Mindestanforderungen an die Passwortqualität sämtlicher Mitarbeiter und Systeme. Diese werden technisch erzwungen.*

Vereinfachte Formulierung: *Stellen Sie technisch sicher, dass Passwörter bestimmte Mindestanforderungen erfüllen (z.B. Länge, Sonderzeichen)?*

A3. Eingeschränkte Rechte zur Administration

Obliegenheit: Zugangssicherung

Relevanz: Nutzerzugänge sollten alle notwendigen Rechte zum Erfüllen der beruflichen Tätigkeit haben. Das Ausführen von Administrationsaufgaben gehört im Regelfall nicht dazu, und ist mit einem erhöhten aktiven und passiven Schadenspotenzial verbunden. Es ist daher *best practice* die alltägliche Arbeit mit weniger privilegierten Accounts durchzuführen.

Standard-Formulierung: *Administrative Zugänge sind ausschließlich Administratoren und ausschließlich zur Erledigung administrativer Tätigkeiten vorbehalten. Die alltägliche Nutzung unserer Systeme findet ohne Administratoren-Privilegien statt.*

Vereinfachte Formulierung: *Sind Administratoren-Rechte ausschließlich Administratoren vorbehalten und nutzen die Administratoren diese Zugänge nur bei administrativen Tätigkeiten?*

A4. Schutz von Servern und mobilen Geräten

Obliegenheit: Zugangssicherung

Relevanz: Server, die über das Internet erreichbar sind, sind dort einem allgemeinen und ständigen Angriffsrisiko ausgesetzt und unterliegen daher höheren Schutzanforderungen als stationäre Büro-Rechner. Zu diesen Maßnahmen können gehören:

- Firewalls
- Zwei-Faktor-Authentifizierung
- Zertifikatsbasierte Anmeldung
- Security-Monitoring und Intrusion Detection oder
- ähnliche Maßnahmen, die einen Fernzugriff erschweren

Hinweis: Die Formulierung „über das Internet erreichbar“ bedeutet, dass das Gerät als *Server* einen Dienst anbietet. Nicht gemeint sind *Clients*, welche zwar das Internet erreichen können, jedoch keine Dienste anbieten.

Mobile Geräte können im Fall eines Diebstahls oder Verlusts in fremde Hände geraten. Ein einfacher Passwortschutz reicht dann nicht mehr aus, um Angreifer am Auslesen der darauf gespeicherten Daten zu hindern. Eine Vollverschlüsselung aller mobilen Datenträger ist daher obligatorisch. Weitere Schutzmaßnahmen können je nach Einsatzzweck

- die Ortung oder Fernlöschung des Geräts
- eine Zwei-Faktor-Authentifizierung bei der Nutzung kritischer Ressourcen oder Zugänge und
- andere Maßnahmen sein, die einen Angreifer am Auslesen von Daten oder dem Zugriff auf kritische Ressourcen hindern

Für die Beantwortung dieser Frage empfiehlt sich eine Matrix aus Schutzmaßnahmen und Geräten, wie beispielhaft in Tabelle 3 dargestellt.

Standard-Formulierung: *Geräte, die über das Internet erreichbar oder im mobilen Einsatz sind, haben wir mit einem zusätzlichen Schutz vor unberechtigtem Zugriff versehen.*

Vereinfachte Formulierung: *Haben Sie Ihre Systeme, die über das Internet erreichbar oder im mobilen Einsatz sind, mit einem zusätzlichen Schutz vor unberechtigtem Zugriff versehen?*

Tabelle 3. Beispielhafte Matrix zur Erfassung von Schutzmaßnahmen für mobile Geräte und Server.

	Sicherheitsmaßnahme			
Geräteklasse	Full-disk-encryption	2-Faktor-Authentifizierung	Security Monitoring	…
Laptop	X		X	
Smartphone		X		
Web-Server			X	
…				

A5. Wöchentliche Datensicherung

Obliegenheit: Datensicherung

Relevanz: Ohne Datensicherung ist eine Wiederherstellung der Betriebsbereitschaft nur schwer möglich, was eine mögliche Betriebsunterbrechung in die Länge zieht. Ein nachhaltiger Datenverlust kann hohe, teils unwiderrufliche Schäden zur Folge haben.

Standard-Formulierung: *Wir schützen uns vor dem Verlust der wichtigsten Unternehmensdaten durch eine mindestens wöchentliche Datensicherung.*

Vereinfachte Formulierung: *Machen Sie mindestens einmal pro Woche eine Sicherungskopie Ihrer Daten?*

A6. Getrennte Aufbewahrung der Datensicherung

Obliegenheit: Datensicherung

Relevanz: Wenn Backup-Systeme dauerhaft mit den Zielsystemen verbunden sind, besteht das Risiko, dass sie bei einem Angriff ebenfalls zu Schaden kommen.

Standard-Formulierung: *Unsere Datensicherungsmedien werden physisch getrennt von den gesicherten Systemen aufbewahrt.*

Vereinfachte Formulierung: *Bewahren Sie Ihre Sicherungskopie physisch getrennt von dem gesicherten System auf?*

A7. Schutz der Datensicherung

Obliegenheit: Datensicherung

Relevanz: Wenn Backups nachträglich vom betroffenen System verändert werden können, besteht das Risiko, dass sie bei einem Angriff ebenfalls zu Schaden kommen. Um dies zu verhindern, können beispielsweise die Sicherungsmedien vom System getrennt werden, wenn keine Sicherung stattfindet. In größeren Netzen ist es üblich, dass Backups von den zu sichernden Systemen durch eigens dafür eingerichteten Sicherungssystem „gezogen“ werden. Von den zu sichernden Systemen besteht dabei kein Schreib- oder Lesezugriff auf die historischen Backup-Daten.

Standard-Formulierung: *Der unberechtigte Zugriff auf die Datensicherungen sowie deren nachträgliche Manipulation werden durch technische Maßnahmen verhindert.*

Vereinfachte Formulierung: *Verhindern Sie die Manipulation oder den unberechtigten Zugriff auf Ihre Sicherungskopien?*

A8. Prüfung der Datensicherung

Obliegenheit: Datensicherung

Relevanz: Eine regelmäßige Überprüfung der Wiederherstellung stellt sicher, dass diese auch im Ernstfall vollständig funktioniert. Findet eine solche regelmäßige Prüfung nicht statt, sind aufgrund des unerprobten Vorgangs Probleme durch Unvollständigkeit oder Verzögerungen bei der Wiederherstellung wahrscheinlicher.

Standard-Formulierung: *Wir stellen durch regelmäßige Tests nach einem festgelegten Turnus sicher, dass unsere Datensicherung und -wiederherstellung funktionieren.*

Vereinfachte Formulierung: *Testen Sie regelmäßig das Wiederherstellen der Daten aus Ihrer Sicherungskopie?*

A9. Sicherheitsupdates

Obliegenheit: Aktueller Stand der Systeme

Relevanz: Mit der Veröffentlichung von Sicherheitsupdates werden auch die zugrundeliegenden Software-Schwachstellen der allgemeinen Öffentlichkeit bekannt. Dadurch steigt das Risiko des Betriebs nicht aktueller Software. In besonders geschäftskritischen Bereichen ist es üblich, Updates zunächst einer Prüfung zu unterziehen, um Probleme im Betrieb auszuschließen. In diesem Fall ist ein zeitnahes Umsetzen je nach Kritikalität des Updates angemessen.

Standard-Formulierung: *Wir stellen sicher, dass alle Systeme auf aktuellem Stand sind und installieren Sicherheitsupdates automatisch oder zeitnah.*

Vereinfachte Formulierung: *Werden Sicherheitsupdates automatisch und zeitnah eingespielt und alle Systeme auf dem aktuellen Stand gehalten?*

A10. Schutz gegen Schadsoftware

Obliegenheit: Schutz gegen Schadsoftware

Relevanz: Wenngleich diese technischen Maßnahmen keine hundertprozentige Sicherheit bieten können, sind sie doch ein relevanter Faktor zur Absicherung der Systeme, insbesondere auch gegen menschliche Fehler.

Hinweis: Ein wirksamer Schutz gegen Schadsoftware erfordert nicht grundsätzlich die Nutzung eines durch Drittanbieter vertriebenen Anti-Viren-Programmes. Moderne Betriebssysteme bieten teilweise wirksamen Schutz mit Bordmitteln. Beispiele sind *Windows Defender* oder die Beschränkung auf Software aus vertrauenswürdigen Quellen mittels *Code Signing*.

Standard-Formulierung: *Alle informationsverarbeitenden Systeme verfügen über einen Schutz gegen Schadsoftware, der automatisch auf dem aktuellen Stand gehalten wird (z.B. Virenscanner, Code Signing, Application Firewall oder ähnlich wirksame Maßnahmen).*

Vereinfachte Formulierung: *Haben alle Computer, Handys und weiteren datenverarbeitenden Systeme einen Schutz gegen Schadsoftware, der automatisch aktualisiert wird?*

Kategorie B

Die folgenden Schutzmaßnahmen gelten für Versicherungsnehmer mit einem Jahresumsatz von mindestens 2 Mio. EUR und höchstens 5 Mio. EUR, sowie Tätigkeit in maximal einem risikobehafteten Geschäftsfeld.

B1. IT-Sicherheitsbeauftragter

Relevanz: IT-Systeme und deren Zusammenspiel in einer größeren Organisation erfordern ein Management mit definierten Verantwortlichkeiten. Der Versicherungsnehmer zeigt durch diese Zuweisung, dass der Bereich IT-Sicherheit mit den notwendigen Ressourcen ausgestattet ist.

Standard-Formulierung: *Es gibt einen Verantwortlichen für die IT-Sicherheit.*

Vereinfachte Formulierung: *Haben Sie einen Verantwortlichen für die IT-Sicherheit benannt?*

B2. Datenschutzbeauftragter

Relevanz: Die Verletzung datenschutzrechtlicher Vorgaben wird von den *Allgemeinen Musterbedingungen des GDV für eine Cyberrisiko-Versicherung* gedeckt. Der Versicherungsnehmer zeigt durch diese Benennung eines Datenschutzbeauftragten, dass die notwendigen Ressourcen und Kapazitäten vorhanden sind, auf die Einhaltung dieser Vorgaben zu achten.

Standard-Formulierung: *Es gibt einen Verantwortlichen für die Einhaltung datenschutzrechtlicher Vorgaben.*

Vereinfachte Formulierung: *Haben Sie einen Verantwortlichen für den Datenschutz benannt?*

B3. Regelmäßige Schulungen

Relevanz: Menschliche Faktoren spielen in der Mehrheit der IT-Sicherheitsvorfälle eine entscheidende Rolle. Wenn technische Schutzmaßnahmen einen Angriff effektiv verhindern, werden Angreifer versuchen, ihr Angriffsziel auf anderem Weg zu erreichen und bedienen sich dabei nicht selten Mitteln der Täuschung. Mitarbeiter sollten daher regelmäßig im Erkennen solcher Angriffsversuche geschult werden.

Standard-Formulierung: *Alle internen und externen Mitarbeiter werden regelmäßig über Maßnahmen zur Informationssicherheit geschult und sind verpflichtet, diese einzuhalten.*

Vereinfachte Formulierung: *Schulen Sie regelmäßig alle internen und externen Mitarbeiter zur Informationssicherheit und verpflichten die Mitarbeiter, die Anforderungen auch einzuhalten?*

B4. „need-to-access“-Prinzip

Relevanz: Durch die konsequente Einschränkung der Nutzerrechte auf die zur Aufgabenerfüllung notwendigen Zugänge wird die Angriffsfläche minimiert, und die Übersicht darüber erhöht.

Standard-Formulierung: *Zugänge für unsere IT-Infrastruktur werden konsequent nur gewährt, wenn sie für die Aufgabenerfüllung notwendig sind.*

Vereinfachte Formulierung: *Gewähren Sie Zugänge zu Ihrer Unternehmens-IT nur dann, wenn sie für eine bestimmte Aufgabe nötig sind?*

B5. Prüfung des „need-to-access“-Prinzips

Relevanz: Während es in vielen Organisationen ein besonders komplexer Vorgang ist, Zugangsrechte überhaupt zu erlangen, werden diese über die Zeit nur akkumuliert und nicht wieder entzogen, wenn der Bedarf nicht mehr besteht. Dadurch wird die Angriffsfläche vergrößert und die Übersicht darüber minimiert. Durch Dokumentation und turnusmäßige Prüfung kann dem entgegengewirkt werden.

Standard-Formulierung: *Administrative Zugänge werden regelmäßig nach einem festgelegten Turnus auf deren Notwendigkeit überprüft.*

Vereinfachte Formulierung: *Überprüfen Sie regelmäßig, ob alle Zugänge für Administratoren noch benötigt werden?*

B6. Verschlüsselter Fernzugriff

Relevanz: Insbesondere die in Hotels und Konferenzzentren üblichen kabellosen Zugänge stellen oft eine unverschlüsselte drahtlose Verbindung zum Netz dar. Sie können von lokalen Angreifern passiv mitgeschnitten oder aktiv manipuliert werden. Der Zugriff auf kritische Systeme darf daher nur über verschlüsselte und authentifizierte Kanäle erfolgen.

Standard-Formulierung: *Der Zugriff auf unsere interne IT-Infrastruktur über öffentliche oder drahtlose Netze erfolgt ausschließlich verschlüsselt.*

Vereinfachte Formulierung: *Verschlüsseln Sie den Datenverkehr, wenn über öffentliche oder drahtlose Netze auf das interne IT-Netz zugegriffen wird?*

B7. Patch Management

Relevanz: Mit der Veröffentlichung von Sicherheitsupdates werden auch die zugrundeliegenden Software-Schwachstellen der allgemeinen Öffentlichkeit bekannt. Dadurch steigt das Risiko des Betriebs nicht aktueller Software.

In einer zunehmend komplexen IT-Infrastruktur kann nicht darauf vertraut werden, dass Anwender ihre Systeme freiwillig und selbstständig warten. Durch zentrales *Patch Management* kann ein homogener aktueller Stand sichergestellt werden.

Die Frage ist für

- Server,
- Arbeitsrechner,
- mobile Geräte und
- weitere Systeme des Versicherungsnehmers

separat in einer Tabelle ähnlich Tabelle 4 zu erfassen.

Tabelle 4. Beispielhafte Matrix zur Erfassung zentral gesteuerter Updates.

	Sicherheitspatches		
Geräteklasse	**Zentral gesteuert**	**Frequenz**	**Realisiert durch**
Laptop	X	14-tägig	AD Policy
Smartphone	X	Innerhalb 24 Stunden	Mobile Device Management
Web-Server	X	Bei CVE-Veröffentlichung	…
…			

Standard-Formulierung: *Die Installation von Sicherheits-Patches für unsere IT wird zentral gesteuert.*

Vereinfachte Formulierung: *Werden Sicherheitsupdates für Ihre Systeme zentral von der IT gesteuert?*

B8. Netzwerk-Separation

Relevanz: Um das Ausbreiten eines Angriffs von einem kompromittierten, wenig kritischen System (z.B. Arbeitsplatzrechner) auf ein kritisches (z.B. Server) zu vermeiden, werden Netzwerke in verschiedene Zonen aufgeteilt, anhand derer kritische Systeme von unkritischen getrennt werden.

Standard-Formulierung: *Unser IT-Netzwerk ist nach Kritikalität der Systeme in unterschiedliche Zonen aufgeteilt.*

Vereinfachte Formulierung: *Ist Ihr IT-Netzwerk je nach Wichtigkeit der Systeme oder Daten für den Betrieb in unterschiedliche Zonen eingeteilt?*

Kategorie C

Die Schutzmaßnahmen für Versicherungsnehmer der Risiko-Kategorie C betreffen primär die organisatorische Sicherheit. Sie werden empfohlen für Versicherungsnehmer mit einem Jahresumsatz von 5 Mio. bis zu 10 Mio. EUR oder Tätigkeit in einem besonderen Bereich erhöhten Risikos.

C1. Verschlüsselter Versand sensibler Daten

Relevanz: Beim Versand von Daten (z.B. via E-Mail) werden diese potenziell unverschlüsselt durch das Netz bewegt und in unverschlüsselter Form auf fremden Servern – auch dauerhaft – vorgehalten. Eine Verschlüsselung, die erst beim Empfänger entschlüsselt wird, minimiert das Risiko des Abgreifens der Daten.

Standard-Formulierung: *Sensible Daten (z.B. personenbezogene Daten und Geschäftsgeheimnisse) werden bei Datenversand verschlüsselt.*

Vereinfachte Formulierung: *Werden sensible Daten wie personenbezogene Daten oder Geschäftsgeheimnisse generell nur verschlüsselt versendet?*

C2. Risikoanalysen

Relevanz: Schwächen in der IT-Sicherheit entstehen nicht nur durch Softwarefehler und können daher auch nicht nur durch Updates behoben werden. Schon bei Systemen geringer Komplexität können einfache Konfigurationsänderungen weitreichende Konsequenzen haben. Durch eine regelmäßige unabhängige Analyse der Systeme können diese und andere Fehler entdeckt und kann auf eine Erhöhung des Sicherheitsniveaus hingearbeitet werden.

Standard-Formulierung: *Für folgende besonders kritische IT-Systeme führen wir regelmäßig Risikoanalysen nach einem festgelegten Turnus durch.*

Vereinfachte Formulierung: *Führen Sie für Ihre besonders kritischen IT-Systeme regelmäßige Risikoanalysen durch?*

Die Systeme und der Turnus sind separat in einer Tabelle ähnlich Tabelle 5 zu erfassen.

Tabelle 5. Beispielhafte Erfassung unabhängiger Sicherheitsüberprüfungen.

	Unabhängige Prüfung		
Geräteklasse	**Turnus**	**Zuletzt**	**Ergebnis**
Laptop	jährlich	MM.JJJJ	8 Findings, 3 kritisch, alle behoben
Smartphone	–	–	–
Web-Server	jährlich	MM.JJJJ	2 Findings, 1 kritisch, alle behoben
…			

C3. IT-Notfall- und -Wiederanlauf-Konzept

Relevanz: Die durch eine Betriebsunterbrechung entstehenden Kosten sind üblicherweise versichert. Der Versicherungsnehmer zeigt durch diese Benennung eines Verantwortlichen für das *Business Continuity Management*, dass die notwendigen Ressourcen und Kapazitäten vorhanden sind, im Falle einer Betriebsunterbrechung zügig und planvoll auf eine Beendigung selbiger hinzuwirken.

Standard-Formulierung: *Unser IT-Notfall- und -Wiederanlauf-Konzept ist schriftlich fixiert und benennt Verantwortliche.*

Vereinfachte Formulierung: *Haben Sie schriftliche IT-Notfall- und IT-Wiederanlauf-Konzepte, in denen konkrete Verantwortliche benannt sind?*

Zusatzfragen E-Commerce

Die folgenden Fragen sind relevant für Versicherungsnehmer, die im Bereich des e-Commerce tätig sind.

EC1. Professionelle Administration

Relevanz: Der selbstständige Betrieb eines Webshops bietet viele technische Fallstricke, die eine überdurchschnittliche technische Kompetenz erfordern. Spezialisierte Dienstleister können oft kürzere Wartungsintervalle und ein höheres allgemeines Sicherheitsniveau gewährleisten.

Standard-Formulierung: *Der Webshop wird selbstständig administriert und betrieben.*

Vereinfachte Formulierung: *Lassen Sie Ihren Webshop von einem Dienstleister oder einer etablierten Plattform administrieren?*

EC2. Keine Speicherung von Kreditkartendaten

Relevanz: Das Speichern von Kreditkartendaten unterliegt den Bedingungen des PCI-DSS und stellt ein hohes Drittschadenrisiko dar.

Standard-Formulierung: *Wir speichern Kreditkartendaten.*

Vereinfachte Formulierung: *Stellen Sie sicher, dass Sie keine Kreditkartendaten speichern?*

EC3. Professionelle Zahlungsabwicklung

Relevanz: Die selbstständige Abwicklung von bargeldlosen Zahlungseingängen bietet viele technische Fallstricke, die eine überdurchschnittliche technische Kompetenz erfordern. Spezialisierte Dienstleister können oft ein höheres allgemeines Sicherheitsniveau und ein geringeres Ausfallrisiko gewährleisten.

Standard-Formulierung: *Wir nutzen einen Payment-Dienstleister zur Abwicklung aller eingehenden bargeldlosen Zahlungsvorgänge.*

Vereinfachte Formulierung: *Nutzen Sie für bargeldlose Zahlungseingänge einen Payment-Dienstleister?*

Zusatzfragen Dienstleister

Überträgt der Versicherungsnehmer informationstechnische Aufgaben an einen Dienstleister, so sind sowohl die Art der Dienstleistung als auch die vertraglichen Bedingungen relevant für eine adäquate Risikoerfassung. Weiterhin ist die Erfassung der verschiedenen Dienstleister relevant für eine Erfassung des Kumulpotenzials.

DL1. Erfassung der Dienstleister

Relevanz: Aus der Art des übergebenen Bereichs werden Abhängigkeits- und Schadenspotenzial bzw. Risikominimierung des Versicherungsnehmers erkenntlich.

Standard-Formulierung: *Der Dienstleister ist in folgenden Bereichen für uns tätig:*

Vereinfachte Formulierung: *Bitte geben Sie an, welche IT-Dienstleister Sie in den folgenden Bereichen in Anspruch nehmen.*

Die Erfassung sollte für jeden Dienstleister, den der Versicherungsnehmer in Anspruch nimmt, separat in einer Tabelle ähnlich Tabelle 6 erfasst werden.

Tabelle 6. Beispielhafte Erfassung von in Anspruch genommenen Dienstleistern.

	Dienstleistung (genau angeben)		
Dienstleister	E-Mail	Hosting	Sonstige (benennen)
Dienstleister 1	X		
Dienstleister 2		X	
Dienstleister 3			Warenwirtschafts-system (Cloud)
…			

DL2. Dienstleistungsvertrag (optional)

Relevanz: Durch fehlende Verfügbarkeit, fehlende Updates und bestehende Sicherheitslücken wird der Versicherungsnehmer einem Risiko ausgesetzt, das potenziell versichert ist.

Hinweis: Es ist davon auszugehen, dass die Bedingungen der Dienstleistung allgemein bekannt und für viele Versicherungsnehmer gleich sind. Weiterhin ist nicht davon auszugehen, dass die Versicherungsnehmer in der Lage sind, die Frage ohne Recherche zu beantworten. Deshalb entfällt die Frage im Online-Fragebogen. Eine Erhebung der Information durch den Erstversicherer ist angeraten.

Standard-Formulierung: *Es existiert ein Dienstleistungsvertrag, in dem Verfügbarkeit, Updates und das Beheben von Sicherheitslücken geregelt sind.*

Vereinfachte Formulierung: *Sind Verfügbarkeit, Updates und das Beheben von Sicherheitslücken in einem Dienstleistungsvertrag geregelt?*

DL3. Zertifizierung und Qualitätssicherung (optional)

Relevanz: Wenngleich die Aussagekraft von Zertifizierungen begrenzt ist, dienen sie als Gradmesser, der Vergleichbarkeit innerhalb einer Branche erlaubt und die Einhaltung von Mindeststandards sicherstellt.

Hinweis: Es ist davon auszugehen, dass die Zertifizierungen der Dienstleister allgemein bekannt sind. Weiterhin ist nicht davon auszugehen, dass die Versicherungsnehmer in der La-

ge sind, die Frage ohne Recherche zu beantworten. Deshalb entfällt die Frage im Online-Fragebogen. Eine Erhebung der Information durch den Erstversicherer ist angeraten.

Standard-Formulierung: *Unser Dienstleister ist zertifiziert oder wir unternehmen regelmäßig eine unabhängige Qualitätssicherung.*

Vereinfachte Formulierung: *Ist Ihr Dienstleister zertifiziert oder unternehmen Sie regelmäßig eine unabhängige Qualitätssicherung?*

DL4. Haftungsfreistellung (optional)

Format: Multiple Choice + offenes Antwortfeld.

Relevanz: Eine Freistellung des Dienstleisters hindert den Versicherer an einem möglichen Regress gegen den Dienstleister und ist daher risikorelevant.

Hinweis: Es ist davon auszugehen, dass die Haftungsbedingungen der Dienstleister allgemein bekannt und für viele Versicherungsnehmer gleich sind. Weiterhin ist nicht davon auszugehen, dass die Versicherungsnehmer in der Lage sind, die Frage ohne Recherche zu beantworten. Deshalb entfällt die Frage im Online-Fragebogen. Eine Erhebung der Information durch den Erstversicherer ist angeraten.

Standard-Formulierung: *Wir haben unseren Dienstleister in den folgenden Fällen von der Haftung freigestellt:*

Vereinfachte Formulierung: *Für welche Fälle haben Sie Ihren Dienstleister von der Haftung freigestellt?*

DL5. Europäisches Datenschutzrecht (optional)

Relevanz: Bspw. ist eine Speicherung von Daten außerhalb des Anwendungsbereichs des europäischen Datenschutzrechts durch einen Dienstleister (Cloud-Anbieter) möglicherweise ein datenschutzrechtlicher Verstoß und kann gegen den Versicherungsnehmer geltend gemacht werden.

Hinweis: Es ist davon auszugehen, dass die rechtlichen Rahmenbedingungen der Dienstleistung allgemein bekannt und für viele Versicherungsnehmer gleich sind. Deshalb entfällt die Frage im Online-Fragebogen. Eine Erhebung der Information durch den Erstversicherer ist angeraten.

Standard-Formulierung: *Unser Dienstleister unterliegt dem einheitlichen Datenschutzrecht der Europäischen Union.*

Vereinfachte Formulierung: *Unterliegt Ihr Dienstleister dem einheitlichen Datenschutzrecht der Europäischen Union?*

Zusatzfragen Private Geräte

Die folgenden Fragen sind relevant für Versicherungsnehmer, die die Nutzung privater Geräte für berufliche Aufgaben genehmigen oder voraussetzen, oder deren Betrieb im Firmennetz (z.B. WLAN) genehmigen.

Hinweis: Bei Versicherungsnehmern der Risiko-Kategorie 1 wird davon ausgegangen, dass diese Fragen negativ beantwortet werden, jedoch auch nur geringe Relevanz haben. Daher werden im Online-Fragebogen diese Zusatzfragen zur Nutzung privater Geräte erst ab der Risiko-Kategorie B gestellt.

PG1. Getrenntes Netz

Relevanz: Da sich private Geräte dem Management durch den Versicherungsnehmer entziehen, kann nicht sichergestellt werden, dass diese das von ihm definierte Sicherheitsniveau einhalten. Die Relevanz der Frage für die Risikoeinschätzung hängt demnach auch davon ab, ob der Versicherungsnehmer ein entsprechendes Niveau überhaupt definiert hat.

Standard-Formulierung: *Private Geräte befinden sich in einem getrennten Netzwerk-Segment*

Vereinfachte Formulierung: *Befinden sich die privaten Geräte in einem getrennten Netzwerk-Segment?*

PG2. Kein Zugriff auf geschäftliche Daten

Relevanz: Die potenziell nicht dem sonstigen Sicherheitsniveau entsprechenden Geräte haben Zugriff auf Firmendaten. Dies ist in vielen kleinen und mittleren Unternehmen üblich und kann nur auf Fall-Basis bewertet werden.

1. Wie kritisch sind die Daten, auf die zugegriffen werden kann?
2. Wie kritisch ist das System, auf das zugegriffen werden kann?

Um einen Überblick über die relevanten Systeme zu erlangen, ist es angeraten, diese tabellarisch aufzustellen. Gängige Dienste sind

- **E-Mail** – je nach Kritikalität des Unternehmens zu tolerieren
- **Interne Dienste** – bei höherer Kritikalität auszuschließen
- **Administration von Servern** – ebenfalls auszuschließen

Standard-Formulierung: *Private Geräte haben Zugriff auf geschäftliche Dienste oder Infrastruktur.*

Vereinfachte Formulierung: *Verhindern Sie, dass über private Geräte auf geschäftliche Dienste oder Daten zugegriffen werden kann?*

Zusatzfragen Datenverarbeitung

Die folgenden Fragen sind relevant für Versicherungsnehmer, die besonders schützenswerte Daten verarbeiten und die Frage E2. Verarbeitung von Daten Dritter bejaht haben.

DV1. Gesetzliche Verschwiegenheitspflichten

Relevanz: Das Speichern und Verarbeiten besonders sensibler Daten unterliegt besonderen gesetzlichen Voraussetzungen. Eine unrechtmäßige Übermittlung oder Kenntnisgabe der in Betracht kommenden Daten löst Informationspflichten der verarbeitenden Stelle aus.

Standard-Formulierung: *Wir verarbeiten Daten, die besonderen gesetzlichen Verschwiegenheitspflichten unterliegen, wie zum Beispiel Gesundheitsdaten.*

Vereinfachte Formulierung: *Verarbeiten oder speichern Sie Daten, die gesetzlichen Verschwiegenheitspflichten unterliegen (z.B. Gesundheitsdaten)?*

DV2. Geschäftsgeheimnisse Dritter

Relevanz: Die Speicherung von Geschäftsgeheimnissen kann ein erhöhtes Drittschadenrisiko darstellen. Dies gilt insbesondere für den Fall, dass auch Vertragsstrafen vom Versicherungsschutz umfasst werden.

Standard-Formulierung: *Wir verarbeiten oder speichern Geschäftsgeheimnisse von Dritten.*

Vereinfachte Formulierung: *Verarbeiten oder speichern Sie Geschäftsgeheimnisse von anderen Firmen?*

DV3. Finanz- oder Steuerdaten Dritter

Relevanz: Eine unrechtmäßige Übermittlung oder Kenntnisgabe dieser Daten löst Informationspflichten der verarbeitenden Stelle aus.

Standard-Formulierung: *Wir verarbeiten oder speichern Finanz- oder Steuerdaten von Dritten.*

Vereinfachte Formulierung: *Verarbeiten oder speichern Sie Finanz- oder Steuerdaten von anderen Firmen oder Personen?*

Zusatzfragen Vernetzte Produktionssysteme (Industrial Control Systems)

Die folgenden Fragen sind relevant für Versicherungsnehmer, die vernetzte Produktionssystem betreiben und die Frage E5. Automatisierte Produktionssysteme bejaht haben.

IC1. Separiertes Netzwerk mit eingeschränktem Zugriff

Relevanz: Die kritischen Produktionssysteme müssen weitestgehend von den sonstigen Arbeitsplätzen und deren Netzwerk separiert sein, um das Ausbreiten einer Infektion in den kritischen Bereich zu erschweren.

Standard-Formulierung: *Die IC-Systeme befinden sich in einem separierten Netzwerk mit eingeschränkten Zugriffsmöglichkeiten.*

Vereinfachte Formulierung: *Befinden sich Ihre automatisierten Produktionssysteme (ICS) in einem separaten Teil des Netzwerks mit beschränkten Zugriffsmöglichkeiten?*

IC2. Fernzugriff nur mit 2-Faktor-Authentifizierung

Relevanz: Ein Fernzugriff auf die vernetzten Produktionssysteme ist generell risikobehaftet und sollte nicht oder nur unter sehr hohen Sicherheitsanforderungen möglich sein.

Standard-Formulierung: *Ein Fernzugriff auf die IC-Systeme ist wenn, dann nur mittels 2-Faktor-Authentifizierung möglich.*

Vereinfachte Formulierung: *Ist ein Fernzugriff auf die Produktionsanlagen ausgeschlossen oder nur nach einer 2-Faktor-Authentifizierung möglich?*

IC3. Sicherheitsmaßnahmen für Terminals

Relevanz: Endgeräte, von denen eine Steuerung oder Konfiguration der ICS erfolgt, haben ein hohes Risiko- und Schadenspotenzial. Für sie sollten daher erhöhte Sicherheits- und Härtungsmaßnahmen Anwendung finden als beispielsweise für einfache Bürogeräte.

Standard-Formulierung: *Für Systeme, die an ICS beteiligt sind, insbesondere auch Terminals, wird die Einhaltung besonderer Härtungsmaßnahmen sichergestellt.*

Vereinfachte Formulierung: *Unterliegen die Steuerungsrechner und andere in die Produktionsanlagen eingebundenen Systeme besonderen Sicherheitsvorgaben? Wird deren Einhaltung regelmäßig geprüft?*

IC4. Erprobte Prozesse zum Einspielen von Updates

Relevanz: Software-Updates bergen immer ein Restrisiko, das System in einen nicht funktionalen Zustand zu versetzen. Dies wird oft zum Anlass genommen, Updates nicht einzuspielen und dadurch die Sicherheit zu mindern. Erprobte Prozesse minimieren das Ausfallrisiko und maximieren die Systemsicherheit.

Standard-Formulierung: *Die Prozesse zum regelmäßigen und unplanmäßigen Einspielen von Sicherheitsupdates sind dokumentiert und erprobt.*

Vereinfachte Formulierung: *Sind die Prozesse für das regelmäßige ebenso wie für das unplanmäßige Einspielen von Sicherheitsupdates dokumentiert und erprobt?*

IC5. Zentrale Protokollierung des Zugriffs

Relevanz: Die Erfassung des Zugriffs ermöglicht auch die regelmäßige Kontrolle auf unberechtigte Nutzung oder gescheiterte Zugriffsversuche und bietet so die Möglichkeit zur frühen Erkennung von Angriffsversuchen.

Standard-Formulierung: *Der Zugriff auf IC-Systeme wird an zentraler Stelle protokolliert und überwacht.*

Vereinfachte Formulierung: *Überwacht und protokolliert eine zentrale Stelle den Zugriff auf Ihre IC-Systeme?*

IC6. Sicherheitsmaßnahmen für mobile Geräte

Relevanz: Für Schutzmaßnahmen der Fragen A1 – A4 gelten auf diesem Kritikalitätslevel erhöhte Anforderungen.

Standard-Formulierung: *Unsere mobilen an dem ICS beteiligten Geräte sind vor unberechtigtem Zugriff durch Verschlüsselung und Passwörter geschützt.*

Vereinfachte Formulierung: *Erlauben Sie den Zugriff auf Ihre Produktionsanlagen von mobilen Geräten grundsätzlich nicht, oder nur wenn diese durch Verschlüsselung und Passwörter geschützt sind?*

IC7. Verschlüsselter Fernzugriff

Relevanz: Für Schutzmaßnahmen der Frage B6. Verschlüsselter Fernzugriff gelten auf diesem Kritikalitätslevel erhöhte Anforderungen.

Standard-Formulierung: *Der Fernzugriff auf IC-Systeme erfolgt ausschließlich auf verschlüsseltem Weg.*

Vereinfachte Formulierung: *Ist ein Fernzugriff auf die Produktionssysteme nur verschlüsselt möglich?*

IC8. Getrennte Aufbewahrung der Datensicherung

Relevanz: Für Schutzmaßnahmen der Fragen A5 – A8 gelten auf diesem Kritikalitätslevel erhöhte Anforderungen.

Standard-Formulierung: *Unsere Datensicherungsmedien werden physisch getrennt von den gesicherten Systemen aufbewahrt.*

Vereinfachte Formulierung: *Bewahren Sie Ihre Sicherungskopien getrennt von dem zu sichernden Produktionssystem auf?*

IC9. Prüfung der Wiederherstellungsprozesse

Relevanz: Für Schutzmaßnahmen der Fragen A5 – A8 gelten auf diesem Kritikalitätslevel erhöhte Anforderungen.

Standard-Formulierung: *Die Prozesse zur Wiederherstellung eines betriebsbereiten Zustandes sind dokumentiert und werden regelmäßig erprobt.*

Vereinfachte Formulierung: *Sind alle Schritte zur Wiederherstellung eines betriebsbereiten Zustands dokumentiert und wird dieser Prozess regelmäßig geprobt?*

IC10. Prüfung der Datensicherung

Relevanz: Für Schutzmaßnahmen der Fragen A5 – A8 gelten auf diesem Kritikalitätslevel erhöhte Anforderungen.

Standard-Formulierung: *Wir stellen durch regelmäßige Tests nach einem festgelegten Turnus sicher, dass unsere Datensicherung und -wiederherstellung funktionieren.*

Vereinfachte Formulierung: *Prüfen Sie regelmäßig, ob Sie die Produktionssysteme aus der Datensicherung wiederherstellen können?*

IC11. Keine Nutzung privater Geräte

Relevanz: Für Schutzmaßnahmen der Frage E4. Nutzung privater Geräte gelten auf diesem Kritikalitätslevel erhöhte Anforderungen.

Standard-Formulierung: *Die Nutzung privater Geräte ist im ICS-Segment nicht gestattet.*

Vereinfachte Formulierung: *Ist die Nutzung privater Geräte im Netzwerk-Segment für die automatisierte Steuerung untersagt?*