**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: August 2017

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 anders als externe Angreifer 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 unterschiedenen, 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 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 diese im Falle eines Angriffs durch Betriebsunterbrechung und Reparaturkosten potenziell hohe Schäden haben.

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 einhergehen. 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 hinaus gehende 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. besondere personenbezogene Daten Dritter i.S.v. BDSG §3(9) o Berufsgeheimnisse o Betriebsgeheimnisse Dritter o ICS
B	▪ Jahresumsatz <= 5 Mio. ▪ *Max. einer* der folgenden Geschäftsbereiche o e-Commerce mit eigener Infrastruktur o Verarbeitung sensibler Daten, insb.: besondere personenbezogene Daten Dritter i.S.v. BDSG §3(9) o Berufsgeheimnisse o Betriebsgeheimnisse Dritter o ICS
C	▪ Jahresumsatz <= 10 Mio.

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 aufgestellt und beträgt 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.

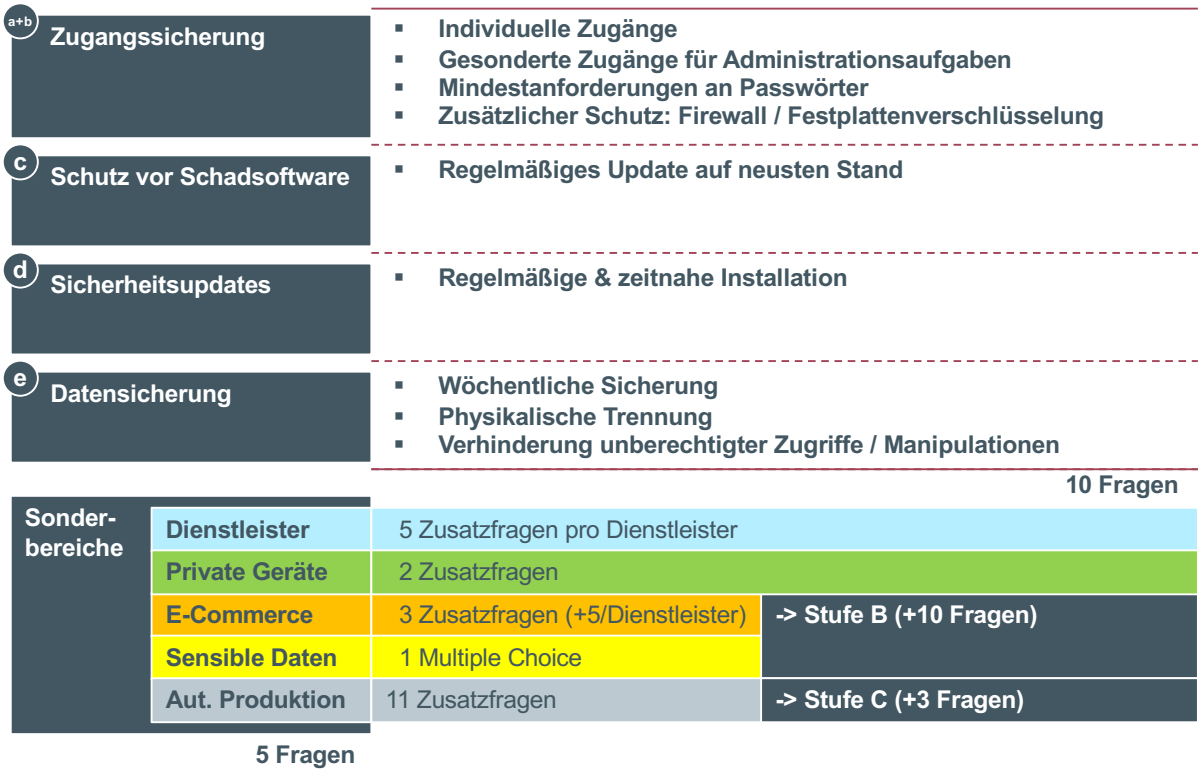

Abbildung 1. Abdeckung der Obliegenheiten und Erfassung der Sonderbereiche.

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 Themenbereich 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.

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.

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. Wir betreiben eine eigene Infrastruktur für Online-Handel (e-Commerce).

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, so sind diese im Rahmen der Zusatzfragen Dienstleister zu erfassen.

E2. Wir speichern und verarbeiten Daten von Dritten.

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.

E3. Wir nutzen einen Dienstleister zur Auftragsdatenverarbeitung nach §11 BDSG.

Relevanz: Laut §11 Bundesdatenschutzgesetz (BDSG) ist der Auftraggeber für die Einhaltung der Vorschriften des BDSG Gesetzes 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.

E4. Die Nutzung privater Geräte ist in unserer Unternehmens-IT gestattet.

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.

E5. Wir nutzen automatisierte Produktionssysteme (ICS).

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.

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. 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.

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.

A2. Wir haben Mindestanforderungen an die Passwortqualität sämtlicher Mitarbeiter und Systeme. Diese werden technisch erzwungen.

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.

A3. Administrative Zugänge sind ausschließlich Administratoren und ausschließlich zur Erledigung administrativer Tätigkeiten vorbehalten. Die alltägliche Nutzung unserer Systeme findet ohne Admin-Privilegien statt.

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.

A4. Geräte, die über das Internet erreichbar, oder im mobilen Einsatz sind, haben wir mit einem zusätzlichen Schutz vor unberechtigtem Zugriff versehen.

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

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 eine

- Ortung oder Fernlöschung des Geräts
- 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.

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. Wir schützen uns vor dem Verlust der wichtigsten Unternehmensdaten durch eine mindestens wöchentliche Datensicherung.

Obliegenheit: Datensicherung

Relevanz: Ohne Datensicherung ist eine Wiederherstellung der Betriebsbereitschaft kaum möglich. Ein nachhaltiger Datenverlust bedeutet darüber hinaus nicht selten einen Schaden von mehreren Personenmonaten.

A6. Unsere Datensicherungsmedien werden physisch getrennt von den gesicherten Systemen aufbewahrt.

Obliegenheit: Datensicherung

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

A7. Der unberechtigte Zugriff auf die Datensicherungen, sowie deren nachträgliche Manipulation werden durch technische Maßnahmen verhindert.

Obliegenheit: Datensicherung

Relevanz: Wenn Backups nachträglich vom betroffenen System verändert werden können, besteht das Risiko, dass sie bei einem Angriff ebenfalls zu Schaden kommen.

A8. Wir stellen durch regelmäßige Tests nach einem festgelegten Turnus sicher, dass unsere Datensicherung und -wiederherstellung funktionieren.

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.

A9. Wir stellen sicher, dass alle Systeme auf aktuellem Stand sind und installieren Sicherheitsupdates automatisch oder zeitnah.

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.

A10. 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).

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.

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. Es gibt einen Verantwortlichen für die IT-Sicherheit.

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.

B2. Es gibt einen Verantwortlichen für die Einhaltung datenschutzrechtlicher Vorgaben.

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 Einhaltung dieser Vorgaben zu achten.

B3. Alle internen und externen Mitarbeiter werden regelmäßig über Maßnahmen zur Informationssicherheit geschult und sind verpflichtet, diese einzuhalten.

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.

B4. Zugänge für unsere IT-Infrastruktur werden konsequent nur gewährt, wenn sie für die Aufgabenerfüllung notwendig sind.

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

B5. Administrative Zugänge werden regelmäßig nach einem festgelegten Turnus auf deren Notwendigkeit überprüft.

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.

B6. Der Zugriff auf unsere interne IT-Infrastruktur über öffentliche oder drahtlose Netze erfolgt ausschließlich verschlüsselt.

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

B7. Die Installation von Sicherheits-Patches für unsere IT wird zentral gesteuert.

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 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	…
…			

B8. Unser IT-Netzwerk ist nach Kritikalität der Systeme in unterschiedliche Zonen aufgeteilt.

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.

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. Sensible Daten (z.B. personenbezogene Daten und Geschäftsgeheimnisse) werden bei Datenversand verschlüsselt.

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

C2. Für folgende besonders kritische IT-Systeme führen wir regelmäßig Risikoanalysen nach einem festgelegten Turnus durch.

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 auf eine Erhöhung des Sicherheitsniveaus hingearbeitet werden.

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. Unser IT-Notfall- und -Wiederanlauf-Konzept ist schriftlich fixiert und benennt Verantwortliche.

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.

Zusatzfragen E-Commerce

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

EC1. Der Webshop wird selbstständig administriert und betrieben.

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.

EC2. Wir speichern Kreditkartendaten.

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

EC3. Wir nutzen einen Payment-Dienstleister zu Abwicklung aller eingehenden bargeldlosen Zahlungsvorgänge.

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.

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. Der Dienstleister ist in folgenden Bereichen für uns tätig:

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

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. Es existiert ein Dienstleistungsvertrag, in dem Verfügbarkeit, Updates und das Beheben von Sicherheitslücken geregelt sind.

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

DL3. Unser Dienstleister ist zertifiziert, oder wir unternehmen regelmäßig eine unabhängige Qualitätssicherung.

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

DL4. Wir haben unseren Dienstleister in den folgenden Fällen von der Haftung freigestellt:

Format: Multiple Choice + offenes Antwortfeld.

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

DL5. Unser Dienstleister unterliegt dem einheitlichen Datenschutzrecht der Europäischen Union.

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 unseren Versicherungsnehmer geltend gemacht werden.

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.

PG1. Private Geräte befinden sich in einem getrennten Netzwerk-Segment

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.

PG2. Private Geräte haben Zugriff auf geschäftliche Dienste oder Infrastruktur.

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

Zusatzfragen Datenverarbeitung

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

DV1. Wir verarbeiten Daten, die besonderen gesetzlichen Verschwiegenheitspflichten unterliegen, wie zum Beispiel Gesundheitsdaten.

Relevanz: Das Speichern und Verarbeiten besonders sensibler Daten unterliegt besonderen Voraussetzungen im Bundesdatenschutzgesetz (BDSG). Eine unrechtmäßige Übermittlung oder Kenntnisgabe der in Betracht kommenden Daten löst unter den Voraussetzungen des § 42a BDSG Informationspflichten der verarbeitenden Stelle aus.

DV2. Wir verarbeiten oder speichern Geschäftsgeheimnisse von Dritten.

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

DV3. Wir verarbeiten oder speichern Finanz- oder Steuerdaten von Dritten.

Relevanz: Eine unrechtmäßige Übermittlung oder Kenntnisgabe dieser Daten löst unter den Voraussetzungen des § 42a BDSG Informationspflichten der verarbeitenden Stelle aus.

Zusatzfragen Vernetzte Produktionssysteme (Industrial Control Systems)

Die folgenden Fragen sind relevant für Versicherungsnehmer, die vernetzte Produktionssystem betreiben, und die Frage E5. Wir nutzen automatisierte Produktionssysteme (ICS) bejaht haben.

IC1. Die IC-Systeme befinden sich in einem separierten Netzwerk mit eingeschränkten Zugriffsmöglichkeiten.

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.

IC2. Ein Fernzugriff auf die IC-Systeme ist wenn, dann nur mittels 2-Faktor-Authentifizierung möglich.

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

IC3. Für Systeme, die an ICS beteiligt sind, insbesondere auch Terminals, wird die Einhaltung besonderer Härtungsmaßnahmen sichergestellt.

Relevanz: Um eine Ausweitung von potenziellen Infektionen zu erschweren, sollte reguläre Arbeitsrechner nicht zur Administration oder Steuerung von vernetzten Produktionssystemen genutzt werden.

IC4. Die Prozesse zum regelmäßigen und unplanmäßigen Einspielen von Sicherheitsupdates sind dokumentiert und erprobt.

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

IC5. Der Zugriff auf IC-Systeme wird an zentraler Stelle protokolliert und überwacht.

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.

IC6. Unsere mobilen an dem ICS beteiligten Geräte sind vor unberechtigtem Zugriff durch Verschlüsselung und Passwörter geschützt.

Relevanz: Für Schutzmaßnahmen der Fragen A1 – A4 (siehe Seite 10) gelten auf diesem Kritikalitätslevel erhöhte Anforderungen.

IC7. Der Fernzugriff auf IC-Systeme erfolgt ausschließlich auf verschlüsseltem Weg.

Relevanz: Für Schutzmaßnahmen der Frage B6. Der Zugriff auf unsere interne IT-Infrastruktur über öffentliche oder drahtlose Netze erfolgt ausschließlich verschlüsselt. gelten auf diesem Kritikalitätslevel erhöhte Anforderungen.

IC8. Unsere Datensicherungsmedien werden physisch getrennt von den gesicherten Systemen aufbewahrt.

Relevanz: Für Schutzmaßnahmen der Fragen A5 – A8 (siehe Seite 11) gelten auf diesem Kritikalitätslevel erhöhte Anforderungen.

IC8. Die Prozesse zur Wiederherstellung eines betriebsbereiten Zustandes sind dokumentiert und werden regelmäßig erprobt.

Relevanz: Für Schutzmaßnahmen der Fragen A5 – A8 (siehe Seite 11) gelten auf diesem Kritikalitätslevel erhöhte Anforderungen.

IC9. Wir stellen durch regelmäßige Tests nach einem festgelegten Turnus sicher, dass unsere Datensicherung und -wiederherstellung funktionieren.

Relevanz: Für Schutzmaßnahmen der Fragen A5 – A8 (siehe Seite 11) gelten auf diesem Kritikalitätslevel erhöhte Anforderungen.

IC10. Die Nutzung privater Geräte ist im ICS-Segment nicht gestattet.

Relevanz: Für Schutzmaßnahmen der Frage E4. Die Nutzung privater Geräte ist in unserer Unternehmens-IT gestattet. gelten auf diesem Kritikalitätslevel erhöhte Anforderungen.