Formular zurücksetzen

Mannheimer Versicherung AG

Fragebogen Cyber-Risiken für Unternehmen ab 10 Mio. Euro Umsatz

Bitte beachten Sie:
Wenn Ihr Unternehmen über mehrere Betriebsstätten verfügt oder wenn andere Unternehmen mitversichert sind, beantworten Sie bitte jede Frage mit der niedrigsten Ausprägung, die auf eine der Betriebsstätten oder eines der mitversicherten Unternehmen zutrifft. Dies stellt sicher, dass das gesamte Risikoprofil Ihres Unternehmens korrekt erfasst wird.

Vermittler-Nummer:

1. Versicherungsnehmer

1.1 Name und Anschrift

1.2 Weitere mitversicherte Gesellschaften (inkl. Unternehmen, welche dieselbe technische Infrastruktur nutzen)

1.3 Homepage (alle Domains) | Statische IP-Adressen

2. Betriebsbeschreibung

Ausführliche Betriebsbeschreibung einschließlich der weiteren Gesellschaften / Unternehmen

3. Allgemeine Informationen

3.1 Jahresumsatz

	im letzten Geschäftsjahr	Anteil E-Commerce
Gesamt	EUR	EUR
davon innerhalb der EU (inklusive Deutschland)	EUR	EUR
davon USA/Kanada	EUR	EUR
davon Rest der Welt	EUR	EUR

3.2 Anzahl Mitarbeiter (inkl. Leiharbeiter)

davon Mitarbeiter in der IT und Informationssicherheit

davon mit Tätigkeiten an Arbeitsplatzcomputern, Servern und Laptops

3.3 Bitte schätzen Sie die Anzahl an eindeutigen Datensätzen innerhalb Ihrer IT

Persönlich identifizierbare Informationen (PII) ☐ bis 10.000 ☐ bis 20.000 ☐ bis 50.000 ☐

Geschützte Gesundheitsinformationen (PHI) ☐ bis 10.000 ☐ bis 20.000 ☐ bis 50.000 ☐

3.4 Wie viele IT-Systeme befinden sich im Unternehmen?

Anzahl Desktop-PCs | Anzahl Laptops | Anzahl Tablets

Anzahl Smartphones | Anzahl Server (physisch)

(virtuell)

3.4.1 Welche Art der Virtualisierung wird in Ihrem Unternehmen eingesetzt?

3.5 Bitte geben Sie die maximale Dauer eines IT-Infrastrukturausfalls (insbesondere des Rechnernetzes) an, die Ihr Unternehmen tolerieren kann, ohne dass es zu kritischen Auswirkungen auf Bereiche wie Liefertermine, Produktqualität oder Unternehmensreputation kommt.

_____ Tage

3.6 **Angaben zum Versicherungsvorschlag**

3.6.1 Gewünschte Versicherungssumme 1.500.000 EUR _____ EUR

3.6.2 Gewünschter Selbstbehalt 5.000 EUR ☐ min. 1 % der Versicherungssumme

4. Informationen zu Datensicherung

4.1 Wie oft führen Sie eine Datensicherung durch? ☐ täglich ☐ wöchentlich ☐ > wöchentlich ☐ unregelmäßig

4.2 Wann wurde der letzte (erfolgreiche) Rücksicherungstest von relevanten/kritischen Systemen durchgeführt? _____

4.2.1 Wurde der Wiederherstellungsprozess dokumentiert? ☐ ja ☐ nein

4.3 In welchen Abständen werden Rücksicherungstests der Systeme durchgeführt? ☐ monatlich ☐ quartalsweise ☐ halbjährlich ☐ jährlich

4.4 Wo werden die Daten gespeichert? (Speichermedium) ☐ Externe Festplatte ☐ Bandsicherung ☐ Cloud-Speicher ☐ NAS / Server ☐ Sonstiges: _____

4.4.1 Cloud-Strukturen

Wie werden Daten und Anwendungen in Ihrer Cloud-Umgebung gesichert? _____

4.5 Sind die Speichermedien von den aktiven IT-Systemen physisch getrennt? ☐ ja ☐ nein, es besteht eine permanente Verbindung

4.6 Ist sichergestellt, dass eine Änderung oder Vernichtung der Datensicherung nicht möglich ist? ☐ ja ☐ nein

4.7 Ist das Backup-System im gleichen Managementsystem (z.B. ActiveDirectory) eingebunden? ☐ ja ☐ nein

4.8 Wie lange werden die Datensicherungen aufbewahrt? _____

4.9 Besteht ein Datensicherungs- und Wiederherstellungskonzept? ☐ ja ☐ nein

4.9.1 Wenn ja: Wurde das Konzept bereits getestet ☐ ja ☐ nein

5. Organisatorische Maßnahmen

5.1 Gibt es einen Verantwortlichen für die IT-Sicherheit (IT-Sicherheitsbeauftragten)? ☐ ja ☐ nein

5.2 Gibt es einen Verantwortlichen für die Einhaltung datenschutzrechtlicher Vorgaben? ☐ ja ☐ nein

5.3 Führen Sie regelmäßig Analysen durch, um festzustellen, ob Sie gegen aktuelle Gefahren geschützt sind? ☐ nein ☐ ISO27001 ☐ BSI - IT Grundschutz ☐ DIN SPEC 27076 ☐ _____

5.4 Werden die Mitarbeiter mindestens jährlich über Maßnahmen zur IT-Sicherheit geschult? ☐ ja ☐ nein

5.5 Existiert ein formaler Prozess für die Zuweisung und den Widerruf von Zugriffsrechten? ☐ ja ☐ nein

5.6 Schränken Sie den Benutzerberechtigungen (Mitarbeiter, Auftragnehmer usw.) auf der Grundlage der geschäftlichen Notwendigkeit des Wissens und der geringsten Rechte ein? ☐ ja ☐ nein

5.7 Klassifizieren Sie Informationen im Hinblick auf die Vertraulichkeit? ☐ ja ☐ nein

5.8 Führen Sie ein aktuelles Bestandsverzeichnis der Software (einschließlich Betriebssysteme, Cloud-Lösungen usw.) und Hardware, die mit Ihrem Netzwerk verbunden sind? ☐ ja ☐ nein

5.9 Verwendet Ihr Unternehmen ein Mobile Device Management (MDM)-System, um die Sicherheit und Verwaltung mobiler Geräte zu gewährleisten? ☐ ja ☐ nein

5.10 Besteht ein IT-Notfall- und -Wiederanlauf-Konzept? ☐ ja ☐ nein

Wenn ja: Werden Verantwortliche im Unternehmen benannt? ☐ ja ☐ nein

Wurde das Konzept bereits getestet? ☐ ja ☐ nein

5.11 Wurden in Ihrem Unternehmen bereits Security Audits, Schwachstellen-analysen (vulnerability assessment) und/oder Penetrationstests durchgeführt? ☐ ja ☐ nein

Wenn ja, in welchem Umfang? _____

6. Zugangsberechtigungen

6.1 Ist für den Zugang zu jedem System eine benutzerindividuelle Kennung/Zugang mit Passwort vergeben? ☐ ja ☐ nein

Wenn nein, gibt es eine Software-Lösung zur Benutzersteuerung mit Kennwort/Passwort? ☐ ja ☐ nein

6.2 Haben Sie Mindestanforderungen an die Passwortqualität sämtlicher Mitarbeiter und Systeme? ☐ ja ☐ nein

Wenn ja, werden diese technisch erzwungen? ☐ ja ☐ nein

6.3 Sind administrative Zugänge ausschließlich Administratoren und ausschließlich zur Erledigung administrativer Tätigkeiten vorbehalten? ☐ ja ☐ nein

6.4 Verfügen Client-Systeme über privilegierte Zugriffsrechte auf Systemebene? ☐ ja ☐ nein

6.5 Wurden lokale Administratorrechte auf Client-Systemen deaktiviert? ☐ ja ☐ nein

6.6 Haben Sie Geräte, die einem erhöhten Risiko ausgesetzt sind mit einem zusätzlichen Schutz vor unberechtigtem Zugriff versehen? ☐ ja ☐ nein

6.7 Haben Sie vom Hersteller voreingestellten Passwörter auf allen Geräten in Ihrem Netzwerk geändert? (z.B. Telefonanlagen, Telefone, Anrufbeantwortern, Drucker, Router, IoT-Geräte) ☐ ja ☐ nein

6.8 Existieren Schutzmaßnahmen wie Einbruchschutz, Zutrittsberechtigungen, unterbrechungsfreie Stromversorgung, etc.? (insbesondere zu/in den Bereichen von kritischen IT-Systemen) ☐ ja ☐ nein

6.9 Wurden Maßnahmen hinsichtlich der Verwendung von USB-Ports getroffen? (z.B. automatische Verschlüsselung, Virenscan, Verbot zur Einbindung von Fremdhardware) ☐ ja ☐ nein

7. Technische Maßnahmen

7.1 Verfügen Sie über ein Patch-Management-Verfahren zur automatischen oder zeitnahen Installation von relevanten Sicherheitsupdates? ☐ ja ☐ nein

Wenn ja, erfolgt die Installation von einer zentralen Stelle innerhalb der IT-Landschaft oder je Endgerät? ☐ zentral ☐ je Endgerät

7.2 Verfügen alle IT-Systeme über einen Schutz gegen Schadsoftware mit automatischen Updates? (z.B. Virenscanner, Code Signing, Endpoint Protection oder ähnliche Maßnahmen) ☐ ja ☐ nein

7.3 **Firewall**

Welche IT-Systeme verfügen über eine Application/Software-Firewall? ☐ alle Systeme ☐ kritische Systeme ☐ Client-Systeme

davon über Betriebssystem ☐ alle Systeme ☐ kritische Systeme ☐ Client-Systeme

davon über Drittanbieter ☐ alle Systeme ☐ kritische Systeme ☐ Client-Systeme

Hersteller: _____

Verfügen Sie über eine Hardware-Firewall? ☐ ja ☐ nein

Wenn ja, Hersteller: _____ Betreut durch: _____

7.4 Wurde das Netzwerk segmentiert? ☐ ja ☐ nein

Wenn ja, in welche Bereiche? ☐ kritische Systeme ☐ Client-Systeme ☐ Sonstige _____

☐ ICS-Systeme ☐ Private Geräte (Mitarbeiter) _____

7.5 Haben Sie eine Network Access Control („NAC“)-Technologie für den Zugriff auf Ihre drahtlosen Unternehmensnetzwerke implementiert? ☐ ja ☐ nein

7.6 Verwenden Sie eine Monitoring-Software zur Überwachung der kritischen IT-Systeme? (z.B. SIEM, Log-Monitoring, Application-Monitoring, Datenbank-Monitoring) ☐ ja ☐ nein

Wenn ja, bitte genauer beschreiben

_____

7.7 **Multi-Faktor-Authentifizierung (MFA)**

7.7.1 Setzt Ihr Unternehmen Multi-Faktor-Authentifizierung (MFA) für den Zugriff auf wichtige Systeme und Daten ein? ☐ ja ☐ nein

7.7.2 Für welche Systeme und Anwendungsbereiche wird MFA verwendet?

_____

7.7.3 Benötigen Administratoren zwingend MFA für den Zugriff auf die internen Server-Systeme und ggf. Cloud-Strukturen? ☐ ja ☐ nein

8. Nutzung privater Geräte / mobile Geräte

8.1 Bieten Sie Ihren Mitarbeitern die Möglichkeit von zu Hause oder mobil zu arbeiten? ☐ ja ☐ nein

Erfolgt der Zugriff ausschließlich mit einer Mehrfachauthentifizierung? (2FA / MFA) ☐ ja ☐ nein

8.2 Sind private Geräte für die Nutzung in Ihrer Unternehmens-IT zulässig (BYOD)? ☐ ja ☐ nein

Wenn ja: Haben die privaten Geräte Zugriff auf die geschäftlichen Dienste oder Infrastruktur? ☐ ja ☐ nein

Wie erhalten die privaten Geräte Zugriff zur Firmen-Infrastruktur?

Gibt es eine Sicherheitsanweisung hinsichtlich der Nutzung von privaten mobilen Geräten innerhalb des Firmennetzwerkes (BYOD) sowie der Nutzung von öffentlichen WLAN-Netzwerken? ☐ ja ☐ nein

9. Dienstleister

9.1 Arbeiten Sie mit externen Dienstleistern zusammen, die mit Ihrem Netzwerk (IT-Infrastruktur) verbunden sind oder die Daten in Ihrem Auftag verarbeiten oder erhalten? ja nein

Wenn ja: Der/die Dienstleister sind/ist in folgenden Bereichen für uns tätig:

9.2 Arbeiten Sie mit einem **externen** IT-Dienstleister zusammen? ☐ ja ☐ nein

Wenn ja: Existiert ein Dienstleistungsvertrag, in dem Verfügbarkeit, Updates und das Beheben von Sicherheitslücken geregelt sind? ☐ ja ☐ nein

Ist der IT-Dienstleister zertifiziert? (z.B. ISO 27001, VdS 10000er, IT-Grundschutz) ☐ ja ☐ nein

Haben Sie die Dienstleister von der Haftung freigestellt? ☐ ja ☐ nein

Wenn ja, in welchen Fällen?

9.3 **Cloud**

9.3.1 Welche Arten von Cloud-Diensten nutzen Sie in Ihrem Unternehmen?

☐ Es werden keine Cloud-Dienste verwendet

☐ Software-as-a-Service (SaaS)

☐ Plattform-as-a-Service (PaaS)

☐ Infrastructure-as-a-Service (SaaS)

9.3.2 Bei welchen Anbietern werden Ihre Cloud-Dienste betrieben?

9.3.3 Für welche Geschäftsprozesse und Datenarten verwenden Sie Cloud-Dienste.

9.3.4 Sind die Cloud-Systeme durch eine DDoS-Protection geschützt? ☐ ja ☐ nein

9.3.5 Wie erfolgt die Überwachung und das Management von Sicherheitsvorfällen in der Cloud?

10. E-Commerce

10.1 Betreiben Sie einen eigenen Online-Handel (E-Commerce)? ☐ ja ☐ nein

Wenn ja: Wird der Webshop selbstständig administriert und betrieben? ☐ ja ☐ nein

Für welche Zielgruppe? ☐ B2B ☐ B2C

Bestehen direkte Verbindungen oder Schnittstellen zu internen Systemen (z.B. Warenwirtschaft, Buchhaltung, Logistikverwaltung)? ☐ ja ☐ nein

10.2 Unterliegen Sie den Anforderungen der Payment Card Industry (PCI) und dem Data Security Service (DSS)? ☐ ja ☐ nein

10.3 Nutzen Sie einen Payment-Dienstleister zu Abwicklung aller eingehenden bargeldlosen Zahlungsvorgänge? ☐ ja ☐ nein

10.4 Speichern Sie Kreditkartendaten? ☐ ja ☐ nein

Wenn ja, wie viele Datensätze?

10.5 Arbeiten Sie mit Kunden, Dienstleistern oder Lieferanten zusammen, die mit Ihrem Netzwerk (IT-Infrastruktur) verbunden sind oder die Daten in Ihrem Auftag verarbeiten oder erhalten? ☐ ja ☐ nein

Wenn ja: Der/die Dienstleister sind/ist in folgenden Bereichen tätig:

Sind die Zugriffe eingeschränkt ☐ ja ☐ nein

Werden die Zugriffe überwacht? ☐ ja ☐ nein

Name der/des Dienstleister/s

10.6 Arbeiten Sie mit einem **externen** IT-Dienstleister zusammen? ☐ ja ☐ nein

Wenn ja: Existiert ein Dienstleistungsvertrag, in dem Verfügbarkeit, Updates und das Beheben von Sicherheitslücken geregelt sind? ☐ ja ☐ nein

Ist der IT-Dienstleister zertifiziert? (z.B. ISO 27001, VdS 10000er, IT-Grundschutz) ☐ ja ☐ nein

Name der/des Dienstleister/s?

Haben Sie die Dienstleister von der Haftung freigestellt? ☐ ja ☐ nein

Wenn ja, in welchen Fällen?

11. Automatisierte Produktionssysteme (ICS) / Operational Technology (OT)

11.1 Verwenden Sie IT-Systeme zur Verwaltung und Steuerung industrieller Abläufe und Anlagen? ☐ ja ☐ nein

Wenn ja:

Sind die Übergänge zu den Systemen durch eine eigene Firewall gesichert und segmentiert? ☐ ja ☐ nein

Ist ein Fernzugriff außerhalb des Unternehmens auf die Verwaltungssysteme oder Anlagen möglich? ☐ ja ☐ nein

Wenn ja: Wurden besondere Sicherheitsmaßnahmen zur Härtung der Systeme ergriffen? ☐ ja ☐ nein

Welche?

Sind die Prozesse zur Wiederherstellung eines betriebsbereiten Zustandes dokumentiert? ☐ ja ☐ nein

Bestehen Vereinbarungen mit den Herstellern bezüglich der Verfügbarkeit von technischen Bauteilen kritischer Anlagen? ☐ ja ☐ nein

Wird der Zugriff auf die Systeme/Anlagen an zentraler Stelle protokolliert und überwacht? ☐ ja ☐ nein

12. Vorversicherung / Vorschaden

Vorversicherung? ☐ ja ☐ nein

Wenn ja: Versicherer

Versicherungs-Nr.

Vertragskündigung erfolgte durch ☐ Versicherungsnehmer oder ☐ Versicherer

Waren Sie bereits von einem Cyber-Schaden betroffen? ☐ ja ☐ nein

Wenn ja, bitte nachfolgende Angaben ergänzen.

Angaben zu Vorschäden (Datum, Anzahl, Art, Schadenhöhe)

Welche Maßnahmen wurden nachträglich ergriffen?

13. Cyber-Risikoanalyse by cysmo®

cysmo® untersucht Ihre IT-Infrastruktur auf Schwachstellen, die von außen sichtbar sind. Da cysmo® nur mit öffentlich einsehbaren Daten arbeitet und einen rein passiven Scan durchführt, entsteht keinerlei Last für Ihre IT-Infrastruktur (wie etwa bei PenTests o. ä.). Der cysmo® Report hilft Ihnen Schwachstellen oder versehentliche Fehlkonfigurationen in Ihrer IT-Infrastruktur zu identifizieren. Diesen Made-in-Germany-Service stellen wir auf Wunsch unseren Kunden, mit Erstellung eines Vorschlags, zur Verfügung.

Möchten Sie den kostenfreien cysmo® Report für Ihr Unternehmen zusammen mit dem Vorschlag erhalten? ☐ ja ☐ nein

14. Bemerkungen / Sonstiges

15. Wichtiger Hinweis

Der Fragebogen dient dem Versicherer zur Risikobewertung und ist Vertragsbestandteil für den zukünftigen Versicherungsschutz. Daher ist es notwendig, dass Sie die in Textform gestellten Fragen wahrheitsgemäß und vollständig beantworten. Eine Verletzung Ihrer vorvertraglichen Anzeigepflicht kann uns zum Rücktritt, zur Kündigung oder zur Vertragsanpassung berechtigen. Unvollständige und unrichtige Angaben können – auch rückwirkend – zum vollständigen oder teilweisen Wegfall des Versicherungsschutzes führen. Bitte beachten Sie hierzu Abschnitt „A) Mitteilung nach § 19 Abs. 5 VVG über die Folgen einer Verletzung der vorvertraglichen Anzeigepflicht‘‘ auf Seite 7 dieses Fragebogens.

Datenschutz

Wir speichern Ihre personenbezogenen Daten, um mit Ihnen kommunizieren zu können. Weitere Informationen hierzu finden Sie unter www.mannheimer.de/datenschutz-kunden.

Ort/Datum

Unterschrift

Risikoträger

Mannheimer Versicherung AG
Augustaanlage 66
68165 Mannheim
Amtsgericht Mannheim HRB 7501

Mitteilung nach § 19 Abs. 5 VVG über die Folgen einer Verletzung der vorvertraglichen Anzeigepflicht

Die nachfolgenden Erläuterungen zur vorvertraglichen Anzeigepflicht gelten sowohl für den Antragsteller als auch ggf. für die mit zu versichernden Personen. Die Anzeigepflicht ist vom Antragsteller – sowohl für sich als auch für die zu versichernde Person – zu beachten und zu erfüllen. Die dann folgenden Hinweise und Informationen über die Rechtsfolgen einer Anzeigepflichtverletzung gelten auch bei einer Pflichtverletzung für eine zu versichernde Person jeweils bezogen auf deren Versicherungsverhältnis.

Damit wir den Versicherungsantrag ordnungsgemäß prüfen können, ist es notwendig, dass die in Textform gestellten Fragen wahrheitsgemäß und vollständig beantwortet werden. Es sind auch solche Umstände anzugeben, denen Sie nur geringe Bedeutung beimessen. Angaben, die Sie nicht gegenüber dem Versicherungsvermittler machen möchten, sind unverzüglich und unmittelbar gegenüber dem jeweiligen Versicherer schriftlich nachzuholen.

Bitte beachten Sie, dass Sie Ihren Versicherungsschutz gefährden, wenn Sie unrichtige oder unvollständige Angaben machen. Nähere Einzelheiten zu den Folgen einer Verletzung der Anzeigepflicht können Sie der nachstehenden Information entnehmen.

Welche vorvertraglichen Anzeigepflichten bestehen?

Sie sind bis zur Abgabe Ihrer Vertragserklärung verpflichtet, alle Ihnen bekannten gefahrerheblichen Umstände, nach denen wir in Textform fragen, wahrheitsgemäß und vollständig anzuzeigen. Wenn nach Ihrer Vertragserklärung, aber vor Vertragsannahme in Textform nach gefahrerheblichen Umständen gefragt wird, sind Sie auch insoweit zur Anzeige verpflichtet.

Welche Folgen können eintreten, wenn eine vorvertragliche Anzeigepflicht verletzt wird?

1. Rücktritt und Wegfall des Versicherungsschutzes

Verletzen Sie die vorvertragliche Anzeigepflicht, können wir vom Vertrag zurücktreten. Dies gilt nicht, wenn Sie nachweisen, dass weder Vorsatz noch grobe Fahrlässigkeit vorliegt. Bei grob fahrlässiger Verletzung der Anzeigepflicht haben wir kein Rücktrittsrecht, wenn wir den Vertrag auch bei Kenntnis der nicht angezeigten Umstände, wenn auch zu anderen Bedingungen, geschlossen hätten. Im Fall des Rücktritts besteht kein Versicherungsschutz. Erklären wir den Rücktritt nach Eintritt des Versicherungsfalls, bleiben wir dennoch zur Leistung verpflichtet, wenn Sie nachweisen, dass der nicht oder nicht richtig angegebene Umstand

- weder für den Eintritt oder die Feststellung des Versicherungsfalls
- noch für die Feststellung oder den Umfang unserer Leistungspflicht

ursächlich war.

Die Leistungspflicht entfällt jedoch, wenn Sie die Anzeigepflicht arglistig verletzt haben. Bei einem Rücktritt steht uns der Teil des Beitrags zu, welcher der bis zum Wirksamwerden der Rücktrittserklärung abgelaufenen Vertragszeit entspricht.

2. Kündigung

Können wir nicht vom Vertrag zurücktreten, weil Sie die vorvertragliche Anzeigepflicht lediglich einfach fahrlässig oder schuldlos verletzt haben, kann der Vertrag unter Einhaltung einer Frist von einem Monat von uns gekündigt werden. Das Kündigungsrecht ist ausgeschlossen, wenn wir den Vertrag auch bei Kenntnis der nicht angezeigten Umstände, wenn auch zu anderen Bedingungen, geschlossen hätten.

3. Vertragsanpassung und Wegfall des Versicherungsschutzes

Können wir nicht zurücktreten oder kündigen, weil wir den Vertrag auch bei Kenntnis der nicht angezeigten Gefahrumstände, wenn auch zu anderen Bedingungen, geschlossen hätten, werden die anderen Bedingungen auf Verlangen Vertragsbestandteil. Haben Sie die Anzeigepflicht fahrlässig verletzt, werden die anderen Bedingungen rückwirkend Vertragsbestandteil, können also für bereits eingetretene Versicherungsfälle zum Wegfall des Versicherungsschutzes führen. Haben Sie die Anzeigepflicht schuldlos verletzt, werden die anderen Bedingungen ab der laufenden Versicherungsperiode Vertragsbestandteil.

Erhöht sich durch die Vertragsänderung der Beitrag um mehr als 10 % oder schließen wir die Gefahrabsicherung für den nicht angezeigten Umstand aus, können Sie den Vertrag innerhalb eines Monats nach Zugang der Mitteilung über die Vertragsanpassung fristlos kündigen. Auf dieses Recht werden wir Sie in einer Mitteilung hinweisen.

4. Ausübung der Rechte

Wir können unsere Rechte zum Rücktritt, zur Kündigung oder zur Vertragsanpassung nur innerhalb eines Monats schriftlich geltend machen. Die Frist beginnt mit dem Zeitpunkt, zu dem wir von der Verletzung der Anzeigepflicht, die das geltend gemachte Recht begründet, Kenntnis erlangt haben. Bei der Ausübung unserer Rechte haben wir die Umstände anzugeben, auf die wir die Erklärung stützen. Zur Begründung können nachträglich weitere Umstände angegeben werden, wenn für diese die Frist nach Satz 1 nicht verstrichen ist. Auf die Rechte zum Rücktritt, zur Kündigung oder zur Vertragsanpassung können wir uns nicht berufen, wenn der nicht angezeigte Gefahrumstand oder die Unrichtigkeit der Anzeige bekannt war.

Die Rechte zum Rücktritt, zur Kündigung und zur Vertragsanpassung erlöschen mit Ablauf von fünf Jahren nach Vertragsschluss. Dies gilt nicht für Versicherungsfälle, die vor Ablauf dieser Frist eingetreten sind. Die Frist beträgt zehn Jahre, wenn Sie die Anzeigepflicht vorsätzlich oder arglistig verletzt haben.

5. Stellvertretung durch eine andere Person

Lassen Sie sich bei Abschluss des Vertrags durch eine andere Person vertreten, so sind bezüglich der Anzeigepflicht, des Rücktritts, der Kündigung, der Vertragsanpassung und der Ausschlussfrist für die Ausübung unserer Rechte die Kenntnis und Arglist Ihres Stellvertreters als auch Ihre Kenntnis und Arglist zu berücksichtigen. Sie können sich darauf, dass die Anzeigepflicht nicht vorsätzlich oder grob fahrlässig verletzt worden ist, nur berufen, wenn weder Ihrem Stellvertreter noch Ihnen Vorsatz oder grobe Fahrlässigkeit zur Last fällt.

Erläuterungen

Administrator Zugang
Ein Administratorzugang gewährt einem Nutzer vollständige und uneingeschränkte Rechte zum Ändern von Systemeinstellungen, Installieren und Entfernen von Software und Zugriff auf alle Dateien im System. Dies ist typischerweise für die Wartung und Verwaltung von IT-Systemen reserviert.

Automatisches Patch-Management-Verfahren
Ein automatisches Patch-Management-Verfahren beinhaltet die systematische Überwachung, Identifizierung und Installation von Softwareupdates (Patches) auf Systemen innerhalb eines Netzwerks, um Sicherheitslücken zu schließen und die Systemleistung zu verbessern.

Backup-Systeme
Verfahren zum Erstellen von Datenkopien zum Schutz vor Datenverlust.

Bandsicherung (Tape Backup)
Eine traditionelle Form der Datensicherung auf Magnetbändern. Geeignet für langfristige Lagerung und große Datenmengen, allerdings mit langsamerem Zugriff verglichen mit Festplatten.

BSI - IT-Grundschutz
Ein Standard des Bundesamtes für Sicherheit in der Informationstechnik (BSI), der Methoden zum Aufbau eines Informationssicherheits-Managementsystem (ISMS), basierend auf vordefinierten Sicherheitsmaßnahmen.

Bring Your Own Device (BYOD)
BYOD steht für „Bring Your Own Device“ und bedeutet, dass Mitarbeiter ihre privaten Geräte wie Smartphones, Tablets oder Laptops für die Arbeit nutzen dürfen.

Cloud-Dienste
Dienstleistungen, die über das Internet verfügbar sind und Speicherplatz, Software oder Rechenleistung bieten. Unterschieden wird zwischen Public Cloud (öffentlich zugänglich), Private Cloud (privat) und Hybrid Cloud (Kombination aus beidem).

Cloud-Speicher
Online-Speicherplatz, der von einem Drittanbieter bereitgestellt wird. Bietet Zugriff von überall und eine einfache Skalierbarkeit. Die Daten werden über das Internet verwaltet und abgerufen.

Datensicherungs- und Wiederherstellungskonzept
Ein Datensicherungs- und Wiederherstellungskonzept umfasst Strategien und Verfahren zur regelmäßigen Sicherung von Daten, um im Falle eines Datenverlustes durch Hardwareausfälle, Softwareprobleme oder Cyberangriffe diese wiederherstellen zu können. Das Konzept sollte folgende Aspekte beinhalten:
- Frequenz der Backups: Bestimmung, wie oft Daten gesichert werden (täglich, wöchentlich, monatlich).
- Speicherorte: Festlegung, wo die Backups gespeichert werden (z.B. externe Festplatten, Cloud-Speicher).
- Testverfahren: Regelmäßige Tests der Wiederherstellungsprozesse, um die Effektivität und die Integrität der Backups zu gewährleisten.
- Verantwortlichkeiten: Zuweisung von Personen oder Teams, die für die Durchführung der Backups und die Wiederherstellung im Notfall verantwortlich sind.

Dedicated Server
Server, die einem einzelnen Mieter zur Verfügung gestellt werden, im Gegensatz zu Shared Hosting, wo mehrere Kunden dieselben Serverressourcen teilen.

DDoS (Distributed Denial of Service)
DDoS ist eine Angriffsart, bei der viele kompromittierte Systeme (oftmals ein Botnetz) verwendet werden, um einen Online-Dienst oder eine Ressource so zu überlasten, dass sie nicht mehr erreichbar ist.

DDoS-Protection
DDoS-Protection bezieht sich auf die Maßnahmen und Technologien, die eingesetzt werden, um einen DDoS-Angriff zu erkennen, abzuwehren und die Auswirkungen auf die betroffenen Ressourcen zu minimieren.

DIN SPEC 27076
Die DIN SPEC 27076 ist ein deutscher Standard für kleine Unternehmen, um deren IT-Sicherheit zu erhöhen. Sie bietet einen „Cyber-Risiko-Check“, der Schwachstellen und Bedrohungen aufdeckt, Risiken bewertet, Gegenmaßnahmen entwickelt und die IT-Sicherheit kontinuierlich verbessert.

E-Commerce
Der elektronische Handel bezieht sich auf den Kauf und Verkauf von Waren oder Dienstleistungen über das Internet.

Externe Festplatte
Ein tragbares Speichergerät, das über USB oder einen anderen Anschluss mit einem Computer verbunden wird. Es bietet eine hohe Speicherkapazität und ist ideal für Backups großer Datenmengen.

Firewall
Sicherheitssystem zum Schutz eines Netzwerks vor unbefugtem Zugriff.

Hardware-Firewall
Eine Hardware-Firewall ist ein physisches Gerät, das zwischen dem Netzwerk eines Unternehmens und externen Netzwerken positioniert wird, um den Netzwerkverkehr zu filtern und unautorisierte Zugriffe zu blockieren.

ICS (Industrial Control Systems)
Steuerungssysteme, die in industriellen Umgebungen zur Automatisierung von Maschinen und Prozessen eingesetzt werden.

ISO 27001
Eine internationale Norm für Informationssicherheits-Managementsysteme (ISMS), die spezifiziert, wie Organisationen ihre Informationen sicher verwalten können.

IT-Infrastruktur (intern / extern)
Interne IT-Infrastruktur bezieht sich auf alle IT-Ressourcen (Hardware, Software, Netzwerke) und Dienste, die innerhalb der Organisation verwaltet und betrieben werden.

Externe IT-Infrastruktur umfasst IT-Ressourcen und Dienste, die von Drittanbietern außerhalb der Organisation bereitgestellt werden, wie Cloud-Dienste oder extern gehostete Server.

IT-Infrastrukturausfall
Bezieht sich auf eine Situation, in der die IT-Systeme eines Unternehmens ganz oder teilweise ausfallen. Dies kann Netzwerke, Server oder andere kritische IT-Komponenten betreffen und führt häufig zu Betriebsunterbrechungen.

IT-Notfall- und -Wiederanlauf-Konzept
Ein IT-Notfall- und -Wiederanlauf-Konzept (auch als Disaster Recovery Plan bekannt) ist darauf ausgelegt, IT-Systeme nach schwerwiegenden Störungen wie Naturkatastrophen, technischen Ausfällen oder Cyberangriffen schnell wiederherzustellen und den Betrieb zu sichern. Wesentliche Elemente dieses Konzepts sind:
- Notfallreaktion: Sofortmaßnahmen nach einem Vorfall, um Schäden zu minimieren und die Sicherheit kritischer Daten zu gewährleisten.
- Wiederherstellungsprozesse: Detaillierte Schritte zur Wiederherstellung der IT-Infrastruktur und kritischer Geschäftsdaten.
- Kommunikationspläne: Vorgehensweisen für die interne und externe Kommunikation während eines Notfalls.
- Regelmäßige Überprüfung und Aktualisierung: Sicherstellen, dass der Plan aktuell bleibt und Änderungen in der IT-Infrastruktur oder im Geschäftsbetrieb reflektiert.

Diese Konzepte sind entscheidend für die Aufrechterhaltung der Betriebskontinuität und die Minimierung von Ausfallzeiten und Datenverlusten in Notfallsituationen.

Lokale Administratorrechte
Lokale Administratorrechte beziehen sich auf die Administratorberechtigungen, die einem Nutzer auf einem einzelnen Gerät (z.B. einem PC oder Laptop) gewährt werden, im Gegensatz zu Netzwerk- oder Systemebenen.

Mobile Device Management (MDM)
Softwarelösungen, die es ermöglichen, mobile Endgeräte wie Smartphones oder Tablets zentral zu verwalten und zu sichern

Monitoring
Monitoring in der IT bezeichnet das kontinuierliche Überwachen von IT-Systemen, Netzwerken und Prozessen, um Leistungsprobleme, Sicherheitsrisiken oder Systemausfälle frühzeitig zu erkennen und darauf reagieren zu können.

Multi-Faktor-Authentifizierung (MFA)
Sicherheitsverfahren, bei dem zur Authentifizierung mehr als ein Nachweis erforderlich ist, z.B. ein Passwort kombiniert mit einem Sicherheitscode, der an ein Smartphone gesendet wird.

NAS (Network Attached Storage)
Ein Dateiserver, der es mehreren Benutzern und Client-Geräten ermöglicht, über ein Netzwerk auf gespeicherte Daten zuzugreifen. Ideal für kleine bis mittelgroße Unternehmen und Heimbüros.

Network Access Control („NAC“)
Network Access Control ist eine Sicherheitstechnik, die den Zugriff auf Netzwerkressourcen steuert und reguliert. Sie überprüft Geräte auf ihre Compliance mit Sicherheitsrichtlinien, bevor sie Zugang zum Netzwerk erhalten.

Operational Technology (OT)
Technologien, die speziell für die Überwachung und Steuerung von Industrieanlagen und -prozessen eingesetzt werden.

PCI DSS (Payment Card Industry Data Security Standard)
Ein Sicherheitsstandard für Organisationen, die Karteninformationen verarbeiten, speichern oder übertragen. Dieser Standard soll Kreditkartenbetrug verhindern und die Datensicherheit verbessern.

Penetrationstests
Simulierte Angriffe auf Systeme und Anwendungen zur Überprüfung der Wirksamkeit der Sicherheitsmaßnahmen.

PHI (Protected Health Information)
Geschützte Gesundheitsinformationen, die spezielle Datenschutzvorschriften erfordern, um die Privatsphäre der Patienten zu schützen.

PII (Personally Identifiable Information)
Persönlich identifizierbare Informationen, die verwendet werden können, um eine einzelne Person zu identifizieren, zu kontaktieren oder zu lokalisieren.

Privilegierte Zugriffsrechte
Privilegierte Zugriffsrechte erlauben Nutzern oder Prozessen erhöhte Berechtigungen, die über die normalen Benutzerrechte hinausgehen, und sind oft notwendig für administrative Aufgaben und kritische Systemänderungen.

Security Audits
Systematische Bewertungen der Sicherheit zur Identifizierung von Schwachstellen und Risiken.

Software-Firewall
Eine Software-Firewall ist ein Programm, das auf einem Computer oder Server läuft, um eingehenden und ausgehenden Netzwerkverkehr zu überwachen und zu kontrollieren, basierend auf vordefinierten Sicherheitsregeln.

Web Application Firewall (WAF)
Eine Web Application Firewall ist eine spezialisierte Form der Firewall, die speziell zum Schutz von Webanwendungen entwickelt wurde. Sie filtert, überwacht und blockiert HTTP-Verkehr zu und von einer Webanwendung, um Angriffe wie SQL-Injection und Cross-Site-Scripting (XSS) zu verhindern.