Fragebogen zum Abschluss einer ERGO Cyber-Versicherung für Unternehmen mit einem Umsatz über 50 Mio. Euro

(Für Unternehmen mit einem Umsatz bis 50 Millionen Euro bitte Fragebogen 50071414 verwenden.)

Agenturinformationen

Name des Vermittlers

Agenturnummer

Bitte senden Sie den ausgefüllten Fragebogen an Ihren Maklerbetreuer oder das Gruppenpostfach: **VHCD@ergo.de**

I. Allgemeine Informationen zum Versicherungsnehmer

1. Name des Antragstellers, ggfs. Rechtsform:

Anrede: ☐ Herr ☐ Frau ☐ Firma ☐ Keine

Titel, Vorname, Zuname/Firma

2. Anschrift:

Straße/Hausnummer

PLZ/Ort

Telefon/E-Mail

Website

Im Rahmen unseres Cyber Frühwarnsystems würden wir Sie gerne proaktiv über Bedrohungen informieren.
Geben Sie hierfür bitte eine passende E-Mail-Adresse (z. B. IT@muster.de) an (freiwillige Teilnahme).

3. Tochterunternehmen/Niederlassung:

(weitere ggf. auf separater Anlage)

4. Branche/Unternehmenstätigkeit:

5. Anzahl Mitarbeiter:

6. Jahresumsatz: (in Euro letztes Geschäftsjahr)

Inland	Europäischer Wirtschaftsraum	USA und Kanada	Übriges Ausland

7. Davon Onlinehandel:

8. Mit welchen Daten (Kunden und Mitarbeiter) arbeiten Sie? (Ein Kunde oder Mitarbeiter entspricht einem Datensatz.)

☐ Personenbezogene Daten — Anzahl der Datensätze

☐ Personenbezogene Gesundheitsdaten — Anzahl der Datensätze

☐ Kreditkartendaten — Anzahl der Datensätze

9. Nutzen Sie Cloud-Computing?

☐ Ja ☐ Beim Anbieter Amazon ☐ Beim Anbieter Google ☐ Beim Anbieter Microsoft

☐ Nein

II. Angaben zum Versicherungsumfang

10. Vorversicherung:

Besteht oder bestand eine Vorversicherung? ☐ Ja ☐ Nein

Wenn ja:

Gesellschaft | Versicherungsschein-Nr. | Beginn | Ablauf

Gekündigt von ☐ Versicherer ☐ Versicherungsnehmer ☐ Noch bestehend

Mit einer Anfrage beim Versicherer erklärt sich der Antragsteller einverstanden: ☐ Ja ☐ Nein

11. Vorschäden:

Gab es in Ihrem Unternehmen in den letzten 5 Jahren Umstände oder Schäden, welche Gegenstand des hier gewünschten Versicherungsschutzes gewesen wären? ☐ Ja ☐ Nein

Falls ja, dann schicken Sie bitte zum Fragebogen die relevanten Unterlagen zum Schadenfall mit. Relevant sind unter anderem die Beschreibung der Schadenursache, die Schadenhöhe und eine Auflistung der eingeführten Maßnahmen zur Prävention zukünftiger Schäden gleicher Art.

12. Gewünschte Versicherungsleistungen:

Pauschale Entschädigungsgrenze in Euro	Selbstbeteiligung in Euro
☐ 1.000.000	☐ 5.000
☐ 3.000.000	☐ 10.000
☐ 5.000.000	☐ 25.000
☐ Andere	☐ Andere

Zusatzbaustein Cyber-Prävention: ☐ Ja ☐ Nein
Für diesen Baustein wird ein Zuschlag von 20 % auf die Jahres-Nettoprämie berechnet.

III. Wichtige Mitteilung zu den Folgen einer Anzeigepflichtverletzung

Werden die im Risikofragebogen gestellten Fragen, soweit sie für die Übernahme der Gefahr erheblich sind, nicht wahrheitsgemäß oder nicht vollständig beantwortet, können wir den Vertrag unter Einhaltung einer Frist von einem Monat kündigen. Bei Vorsatz oder grober Fahrlässigkeit können wir sogar von dem Vertrag zurücktreten. Sie haben dann von Anfang an keinen Versicherungsschutz, es sei denn, durch die Verletzung der Anzeigepflicht ist uns kein Nachteil entstanden. Unser Rücktritts- und Kündigungsrecht ist – außer bei Vorsatz – ausgeschlossen, wenn wir den Vertrag auch bei Kenntnis der nicht angezeigten Umstände, wenn auch zu anderen Bedingungen, geschlossen hätten. Die Vertragsanpassung, etwa in Form eines Risikoausschlusses oder einer Beitragserhöhung, wird auf unser Verlangen rückwirkend, bei einer von Ihnen nicht zu vertretenden Pflichtverletzung ab der laufenden Versicherungsperiode wirksam. Durch die rückwirkende Einfügung eines Risikoausschlusses kann Ihr Versicherungsschutz für einen eingetretenen oder zukünftigen Versicherungsfall ebenfalls entfallen.

IV. Informationen zur IT-Sicherheit

Im folgenden Kapitel werden Fachbegriffe benutzt. Diese sind mit einem Sternchen* markiert. Eine entsprechende Erläuterung finden Sie auf der letzten Seite im Glossar.

1. Organisatorisches

1.1 Haben Sie ein Information Security Management System (ISMS*) etabliert? ⓘ

☐ Ja ☐ Nein, aber eine formelle IT-Sicherheitsrichtlinie ☐ Nein

ERGO

1.2 Haben Sie einen Verantwortlichen für die Informationssicherheit (z. B. CISO*) benannt?

☐ Ja ...
  ☐ ... und dieser berichtet direkt an die Geschäftsführung
  ☐ ... und die Stelle ist funktional von der IT-Abteilung getrennt?
☐ Nein

1.3 Kreuzen Sie an, für welche Standards Sie auditiert sind bzw. über ein gültiges Zertifikat verfügen. (Mehrfachantwort möglich)

☐ ISO 27001
☐ BSI Grundschutz
☐ NIST Cybersecurity Framework
☐ Keine Standards vorhanden oder auditiert
☐ Andere (bitte im Notizfeld aufführen)

1.4 Kreuzen Sie an, welche Richtlinien Ihr Rollen- und Rechtekonzept vorschreibt. (Mehrfachantwort möglich)

☐ Administrative Konten werden ausschließlich für die Nutzung von administrativen Tätigkeiten verwendet
☐ Jeder Nutzer nutzt ausschließlich sein individuelles Benutzerprofil (keine Shared User Accounts*)
☐ Die Passwörter der administrativen Konten sind in einem Passwort Safe* aufbewahrt
☐ Es gibt einen formalen Prozess für die Zuweisung und den Widerruf von Zugriffsrechten
☐ Die Zugriffsmöglichkeiten der Benutzerprofile auf die IT-Systeme sind auf das Nötigste beschränkt
☐ Die Mitarbeiter (ausgenommen die IT-Administratoren) verfügen nicht über lokale Adminrechte
☐ Keine der Anforderungen wird vollständig erfüllt oder es gibt keine Richtlinie

1.5 Für welche Geräte nutzen Sie eine Mobile Device Management Lösung (MDM)*? (Mehrfachantwort möglich)

☐ Smartphones und Tablets
☐ Laptops
☐ Wird nicht genutzt

1.6 In welchen Abständen spielen Sie Sicherheitsupdates auf Ihren IT-Systemen (Hard- und Software) ein? (Mehrfachantwort möglich)

☐ Kritische Sicherheitsupdates innnerhalb von 7 Tagen
☐ Restliche Sicherheitsupdates innerhalb von 30 Tagen
☐ Später oder gar nicht

1.7 Verfügen Sie über ein aktuelles Inventarverzeichnis an Software- (einschl. Betriebssystemen) und Hardware-Beständen in Ihrem Netzwerk?

☐ Ja
☐ Nein

1.8 Wie schützen Sie Altsysteme, die nicht mehr vom Hersteller mit Sicherheitsupdates versorgt werden? (Mehrfachantwort möglich)
Sollten Sie noch Altsysteme verwenden, dann ergänzen Sie bitte im Notizfeld, wozu diese Systeme verwendet werden.

☐ Keine Altsysteme vorhanden
☐ Separates Netz (keine Verbindung zu allen anderen Netzwerken)
☐ Netzwerksegmentierung* inkl. Firewall
☐ Überwachung des Datenverkehrs*
☐ Kein Internetzugang
☐ Eine vollständige Ablösung der Altsysteme ist geplant bis zum: _____

1.9 Welche Voraussetzungen erfüllt Ihre Kennwortrichtlinie? (Mehrfachantwort möglich)

☐ Mindestens 8 Zeichen UND mindestens ein Buchstabe, eine Ziffer und ein Sonderzeichen
☐ Die Einhaltung hinsichtlich der Passwortqualität wird technisch erzwungen
☐ Alle Mitarbeiter verwenden einen Passwort Safe bzw. Passwort Manager*
☐ Keine Voraussetzung ist komplett erfüllt oder es gibt keine Richtlinie

1.10 Ist das Ausführen von Makro-Programmen* für Office-Anwendungen eingeschränkt?

☐ Ja
☐ Nein

1.11 Nutzen Sie einen Threat Intelligence Anbieter*, der Sie über neueste Bedrohungen und Sicherheitslücken informiert?

☐ Ja
☐ Nein

1.12 Wie gehen Sie mit Informationssicherheitsvorfällen (IT-Sicherheit und Datenschutz)* um? (Mehrfachantwort möglich)

☐ Werden an zentraler Stelle gesammelt und je nach Kritikalität schnellstmöglich behoben
  ☐ und es werden Maßnahmen zur Prävention aus den Vorfällen abgeleitet
☐ Es existiert ein einheitlicher Meldeprozess, über den jeder Mitarbeiter informiert ist
☐ Es gibt kein standardisiertes Verfahren

1.13 Kreuzen Sie an, wie Sie Schwachstellen erkennen und beheben. (Mehrfachantwort möglich)

☐ Automatische Schwachstellenscans mindestens alle 2 Jahre
☐ Externer Penetrationstest mindestens alle 2 Jahre
☐ Behebung der gefundenen Schwachstellen, die eine kritische Auswirkung auf die IT-Sicherheit haben
☐ Schwachstellen werden nicht systematisch überprüft/gefunden

ERGO

1.14 Welche Anforderungen erfüllt Ihre Regelung zum Umgang mit externen Datenträgern?

☐ Die Nutzung externer Datenträger ist nicht zugelassen
☐ Die Datenträger werden vor der Benutzung auf Schadprogramme geprüft
☐ Keine der genannten Anforderungen ist erfüllt

Notizfeld nur **digital und nicht handschriftlich** ausfüllen
Anmerkung zu Frage 1.1
Anmerkung zu Frage 1.1
Anmerkung zu Frage 1.1

2. Compliance und Datenschutz

2.1 Haben Sie ein Verfahren implementiert, um alle datenschutzrelevanten gesetzlichen, behördlichen und vertraglichen Anforderungen dauerhaft zu erfüllen?

☐ Ja ☐ Nein

2.2 Haben Sie einen Datenschutzbeauftragten (intern oder extern) bestellt?

☐ Ja ☐ Nein

2.3 Welche Richtlinien überprüfen Sie (intern oder extern) regelmäßig (mindestens alle 2 Jahre) durch Audits? (Mehrfachantwort möglich)

☐ Informationssicherheitsrichtlinie ☐ Keine der genannten
☐ Datenschutzrelevante Anforderungen

2.4 Erfordern Vereinbarungen mit Drittanbietern ein Sicherheitsniveau, das Ihrem eigenen Standard für Informationssicherheit entspricht?

☐ Ja ☐ Nein

2.5 Verschlüsseln Sie gespeicherte, sensible/vertrauliche Daten (z. B. On-Premises, auf mobilen Geräten und/oder in der Cloud)?

☐ Ja ☐ Nein

Notizfeld nur **digital und nicht handschriftlich** ausfüllen
Anmerkung zu Frage 2.1
Anmerkung zu Frage 2.1
Anmerkung zu Frage 2.1

3. Personal

3.1 Kreuzen Sie an, welche Anforderungen Ihre Weiterbildungen zum Thema Informationssicherheit (Awareness Schulungen) erfüllen. (Mehrfachantwort möglich)

☐ Die Schulungen sind verpflichtend für alle Mitarbeiter mit Zugang zu IT-Systemen
☐ Es wird geprüft und dokumentiert, dass die Schulungen mindestens jährlich durchgeführt werden
☐ Die Schulungen umfassen unter anderem Social Engineering, aktuelle Cyber-Bedrohungen und Grundlagen der IT-Sicherheit
☐ Die Schulungen sind auch auf verschiedene berufliche Funktionen ausgelegt (z. B. extra Schulungen für das Personalwesen, Führungskräfte oder Rechnungswesen)
☐ Zusätzlich zur Schulung werden Phishing-Kampagnen* jährlich durchgeführt
☐ Keine der genannten Anforderungen wird erfüllt

3.2 Sind private Geräte für dienstliche Zwecke verboten? (Mehrfachantwort möglich)

☐ Ja
☐ Nein, ...
  ☐ ... aber es muss ein Mobile Device Management* auf dem Gerät installiert sein
  ☐ ... aber es gibt eine entsprechende Richtlinie zum sicheren Umgang

Notizfeld nur **digital und nicht handschriftlich** ausfüllen
Anmerkung zu Frage 3.1
Anmerkung zu Frage 3.1
Anmerkung zu Frage 3.1

ERGO

4. Technische Maßnahmen

4.1 Kreuzen Sie an, welche Anforderungen Ihre Firewalls erfüllen. (Mehrfachantwort möglich)

- ☐ Die Firewalls sind hinsichtlich der entsprechenden Anwendungszwecke konfiguriert*
- ☐ Alle Internetzugangspunkte sind durch Firewalls abgesichert
- ☐ Die Konfiguration aller Firewalls wird anlassbezogen, aber mindestens jährlich auf Aktualität überprüft
- ☐ Keine der Anforderungen ist erfüllt

4.2 Kreuzen Sie an, welche Anforderungen Sie im Hinblick auf Schutz vor Schadsoftware erfüllen. (Mehrfachantwort möglich)

- ☐ Ein Antimalwareprogramm ist auf allen Clients vorhanden
- ☐ Ein Antimalwareprogramm ist auf allen Servern vorhanden
- ☐ Das Antimalwareprogramm arbeitet mit Anomalieerkennung bzw. verhaltensbasierter Erkennung
- ☐ Keine der Anforderungen ist erfüllt

4.3 Kreuzen Sie an, welche Maßnahmen Sie zur Angriffserkennung verwenden. (Mehrfachantwort möglich)

- ☐ Intrusion Detection System (IDS)*
- ☐ Intrusion Prevention System (IPS)*
- ☐ Nutzung eines Systems zur Erfassung von sicherheitsrelevanten Vorfällen (SIEM)*
- ☐ Nutzung eines Security Operation Center (SOC)*
- ☐ Keine der Anforderungen ist erfüllt

4.4 Wie sichern Sie Ihre Fernzugriffe (kein Site-to-Site)* ab? (Mehrfachantwort möglich)

- ☐ Nutzung VPN
- ☐ IP-Sperrlisten (Black-List)
- ☐ Geographische Einschränkungen von IP-Adressen
- ☐ Keine der Anforderungen ist erfüllt

4.5 Kreuzen Sie an, welche Bereiche in Ihrem Netzwerk segmentiert werden. (Mehrfachantwort möglich)

- ☐ Demilitarisierte Zone (DMZ)*
- ☐ Standorte
- ☐ Internet of Things (IoT)
- ☐ Telefonanlage
- ☐ Hochkritische Bereiche (z. B. Produktion (OT) oder Point of Sale)
- ☐ Clients und Server
- ☐ Drucker
- ☐ Keine Segmentierung vorhanden

4.6 Kreuzen Sie an, welche Schritte Sie zur Systemhärtung* durchführen. (Mehrfachantwort möglich)

- ☐ Deaktivierung von ungenutzen Ports auf kritischen IT-Systemen
- ☐ Deaktivierung von für den Betrieb nicht zwingend erforderlichen Softwarekomponenten auf kritischen IT-Systemen
- ☐ Gehärtete Basiskonfiguration von Clients*
- ☐ Keine der Anforderungen ist erfüllt

4.7 Welche Zugänge/Systeme sichern Sie durch einen zweiten Faktor (2FA/MFA) ab? (Mehrfachantwort möglich)

- ☐ Alle Cloud-Zugänge
- ☐ Alle administrativen Systeme
- ☐ Alle Fernzugriffe (ohne Site-to-Site) auf die eigenen IT-Systeme
- ☐ Keine

Notizfeld nur **digital und nicht handschriftlich** ausfüllen

Anmerkung zu Frage **4.1**

Anmerkung zu Frage **4.1**

Anmerkung zu Frage **4.1**

5. Backup und Notfallmanagement

5.1 Kreuzen Sie an, welche Anforderungen Ihre Backup-Strategie erfüllt. (Mehrfachantwort möglich)

- ☐ Mindestens wöchentliche Sicherung aller geschäftsrelevanten Daten
  - ☐ Die mindestens wöchtentliche Sicherung ist eine Volldatensicherung (nicht inkrementell)
- ☐ Anwendung der 3-2-1 Regel*
- ☐ Die Backups sind durch einen Angreifer nicht mehr veränderbar (z. B. immutable Storage* oder offline)
- ☐ Keine der Anforderungen ist erfüllt

5.2 Werden Ihre Backups getrennt von den restlichen Domänen (außerhalb des Active Directory*) aufbewahrt?

- ☐ Ja
- ☐ Ja und offline
- ☐ Nein

5.3 Wie lange bewahren Sie Ihre Backups auf?

- ☐ Mindestens 30 Tage
- ☐ Mindestens 180 Tage
- ☐ Mindestens 360 Tage
- ☐ Kürzer als die genannten Optionen

ERGO

5.4 Testen Sie die korrekte Rücksicherbarkeit Ihrer Backups regelmäßig (mindestens alle 6 Monate) automatisiert oder manuell?

☐ Ja, vollständig
☐ Ja, stichprobenartig
☐ Nein

5.5 Kreuzen Sie an, welche Anforderungen Ihr Plan zur Reaktion auf kritische Informationssicherheitsvorfälle (Notfallplan) erfüllt. (Mehrfachantwort möglich)

☐ Ist physisch vorhanden und den Schlüsselpersonen bekannt
☐ Wird mindestens jährlich überprüft
☐ Wird mindestens jährlich in einer Notfall-Übung geprobt
☐ Notfallplan nicht vorhanden

5.6 Kreuzen Sie an, welche Anforderungen Ihr Plan zur Geschäftsaufrechterhaltung (Business Continuity Management) erfüllt. (Mehrfachantwort möglich)

☐ Ist physisch vorhanden und den Schlüsselpersonen bekannt
☐ Wird mindestens jährlich überprüft
☐ Wird mindestens jährlich durch Cyberangriffs-Szenarien geprobt
☐ Recovery Time Objectives (RTO)* and Recovery Point Objectives (RPO)* auf der Grundlage von Kritikalitätslevel* des jeweiligen Systems / der jeweiligen Anwendung definiert
☐ Plan ist nicht vorhanden

Notizfeld nur **digital und nicht handschriftlich** ausfüllen
Anmerkung zu Frage 5.1
Anmerkung zu Frage 5.1
Anmerkung zu Frage 5.1

6. Zusatzfragen

6.1 Verwenden Sie Software der Firma Kaspersky?

☐ Ja
☐ Nein

6.2 Wenn ja: Ist geplant, diese in den nächsten 3 Monaten abzulösen?

☐ Ja
☐ Nein

7. Die folgenden Fragen müssen Sie nur beantworten, wenn Sie OT* verwenden. ☐ Zutreffend ☐ Nicht zutreffend

7.1 Ist Ihre IT von der OT getrennt?

☐ Ja
☐ Nein
☐ Ja und einzelne OT-Bereiche sind zusätzlich untereinander getrennt

7.2 Wie wird auf Ihre OT zugegriffen?

☐ Ausschließlich lokal
☐ Fernzugriffe durch Betriebszugehörige
☐ Fernzugriffe durch Dritte

7.3 Wie werden Fernzugriffe auf die OT abgesichert? (Mehrfachantwort möglich)

☐ Multifaktorauthentifizierung (MFA)
☐ Whitelisting*
☐ VPN
☐ Es gibt keine Fernzugriffe

7.4 Kann Ihre OT auch ohne Zugriff auf die IT produzieren?

☐ Ja
☐ Nein

Notizfeld nur **digital und nicht handschriftlich** ausfüllen
Anmerkung zu Frage 6.1
Anmerkung zu Frage 6.1
Anmerkung zu Frage 6.1

8. Die folgenden Fragen müssen Sie nur beantworten, wenn Sie IT-Dienstleister sind. ☐ Zutreffend ☐ Nicht zutreffend

8.1 Haben Sie eine Berufshaftpflichtversicherung für IT-Dienstleister?

☐ Ja ☐ Nein

Wenn ja:

Gesellschaft | Versicherungsschein-Nr. | Versicherungssumme für Vermögensschaden-Haftpflichtschäden

Beginn | Ende

8.2 Bitte geben Sie an, welche Tätigkeiten Sie ausführen. (Anteil am Gesamtumsatz auf volle 10 % runden)

8.2.1 Hosting von IT-Systemen (Serverdienstleistung)

☐ Nein ☐ Ja, Anteil: ___%

8.2.2 Bereitstellung von Anything-as-a-Service (XaaS) Angeboten, wie z. B. Software-as-a-Service oder Plattform-as-a-Service

☐ Nein ☐ Ja, Anteil: ___%

8.2.3 Inbetriebnahme von IT-Systemen

☐ Nein ☐ Ja, Anteil: ___%

8.2.4 IT-Beratung

☐ Nein ☐ Ja, Anteil: ___%

8.2.5 Software-Entwicklung

☐ Nein ☐ Ja, Anteil: ___%

8.2.6 Customizing von Soft- oder Hardware

☐ Nein ☐ Ja, Anteil: ___%

8.2.7 Handel mit nicht selbst hergestellter Hard- und/oder Software (inkl. Verkaufsberatung)

☐ Nein ☐ Ja, Anteil: ___%

8.2.8 Netzwerktechniker

☐ Nein ☐ Ja, Anteil: ___%

8.2.9 Sonstige Leistungen (bitte im Notizfeld aufführen)

☐ Nein ☐ Ja, Anteil: ___%

Notizfeld nur **digital und nicht handschriftlich** ausfüllen

Anmerkung zu Frage 8.2.1

Anmerkung zu Frage 8.2.1

Anmerkung zu Frage 8.2.1

V. Unterschrift und Bestätigungen

Der/Die Unterzeichner/-in erklärt mit Wirkung für und gegen die Gesellschaft als Versicherungsnehmer, ihre Tochterunternehmen/ Niederlassungen, die obigen Fragen vollständig und wahrheitsgemäß beantwortet zu haben.

Datum | Antragsteller (Vertretungsberechtigter) | Vermittler/ORGA

ERGO

VI. Begriffserklärung/Glossar

1.1	Ein **Information Security Management System (ISMS)** hilft Unternehmen, sich vor IT-Sicherheitsvorfällen zu schützen und IT-Risiken zu vermeiden. Dazu bietet ein ISMS verschiedene Verfahren und Tools, die in der Regel die Informationssicherheit des ganzen Unternehmens erhöhen.
1.2	Ein **Chief Information Security Officer (CISO)** ist für die Informationssicherheit im Unternehmen ganzheitlich verantwortlich.
1.4	**Shared User Accounts** sind Nutzerkonten, die von verschiedenen Mitarbeitern benutzt werden. Alle Nutzer kennen die Login-Daten des Shared User Accounts. Ein **Passwort Safe** bzw. Passwort Manager dient zur sicheren Verwaltung von Passwörtern.
1.5	Ein **Mobile Device Management (MDM)** ermöglicht die Durchsetzung von Richtlinien auf dem jeweiligen Gerät. So kann beispielsweise sichergestellt werden, dass immer die aktuellste Version installiert ist.
1.8	Bei der **Netzwerksegmentierung** wird das Altsystem in einem extra Netzwerksegment betrieben. Das Segment ist mindestens durch eine Firewall, die sehr streng konfiguriert ist, geschützt. Bei der **Überwachung des Datenverkehrs** wird der aus- und eingehende Datenverkehr auf Anomalien untersucht. Dadurch kann ein Angriff schnellstmöglich festgestellt werden.
1.9	Ein Passwort Safe bzw. **Passwort Manager** dient zur sicheren Verwaltung von Passwörtern.
1.10	Ein **Makro-Programm** für Office-Anwendungen ist eine Arbeitserleichterung, da etliche Aktionen automatisch ausgeführt werden können. Allerdings können Makro-Programme auch als Schadcode missbraucht werden.
1.11	**Threat Intelligence Anbieter** durchsuchen das Internet tagtäglich nach neuen Cyber-Bedrohungen. Hat man solch einen Service abonniert, dann wird man vor neuen Angriffen gewarnt, die zu den eigenen IT-Systemen passen.
1.12	Zu Informationssicherheitsvorfällen zählen jegliche Vorkommnisse, die als ein **IT-Sicherheitsvorfall** oder eine **Datenschutzverletzung** eingeordnet werden können.
3.1	Bei **Phishing Kampagnen** werden E-Mails verschickt, die Phishing-Mails stark ähneln. Fällt ein Nutzer auf eine solche E-Mail rein, dann bekommt er einen Hinweis und eine entsprechende Schulung. Durch solche Kampagnen werden Mitarbeiter praxisnah geschult, Phishing-Mails erkennen zu können.
3.2	Ein **Mobile Device Management (MDM)** ermöglicht die Durchsetzung von Richtlinien auf dem jeweiligen Gerät. So kann beispielsweise sichergestellt werden, dass immer die aktuellste Version installiert ist.
4.1	Eine **Firewall** funktioniert nur dann wie gewünscht, wenn ein entsprechendes Regelwerk hinterlegt ist. Diese Regeln müssen auf den jeweiligen Anwendungszweck angepasst werden. Die voreingestellten Standardregeln genügen oftmals nicht.
4.3	Ein **Intrusion Detection System (IDS)** dient zur Erkennung von Angriffen auf einem System. Ein **Intrusion Prevention System (IPS)** erkennt Angriffe und wehrt diese proaktiv ab. Ein **Security Information und Event Management (SIEM)** dient als zentrale Anlaufstelle zur Erfassung und Sammlung von Cybervorfällen. Ein **Security Operation Center (SOC)** ist eine zentrale Überwachungseinheit, die durch menschliches Eingreifen Angriffe abwehren kann.
4.4	**Site-to-Site** bezeichnet den Bereich zwischen zwei Unternehmensstandorten.
4.5	Eine **Demilitarisierte Zone (DMZ)** bezeichnet den Bereich zwischen externen (z. B. Internet) und internen Netzwerken. Typischerweise ist diese Zone z. B. durch Firewalls besonders gesichert.
4.6	Eine **Systemhärtung** ist die Anpassung eines IT-Systems, sodass dieses ein höheres Schutzniveau aufweist (also gehärtet ist). Die **gehärtete Basiskonfiguration** von Clients beschreibt einen Auslieferungszustand von Endgeräten, der ein höheres Schutzniveau als das der Hersteller aufweist.
5.1	Die **3-2-1 Backup Regel** beschreibt eine Datensicherungsstrategie. Dabei sind drei Kopien insgesamt vorhanden, welche auf zwei verschiedenen Systemen gespeichert werden, wobei ein System außerhalb des Unternehmens liegt. Ein **immutable Storage** ist eine Speicherform, die keine Änderung an den Daten zulässt. Somit kann ein Angreifer das Backup nicht manipulieren bzw. löschen.
5.2	Ein **Active Directory (AD)** dient zur Verwaltung und Steuerung von Objekten und Ressourcen. Oftmals bildet das AD die Unternehmensstruktur inklusive aller Geräte und Ressourcen ab.
5.6	Die **Recovery Time Objevtices (RTO)** beschreiben, wie lange ein System maximal ausfallen kann, bevor ein signifikanter Schaden entsteht. Die **Recovery Point Objectives (RPO)** beschreiben, wie viele Daten einem System maximal fehlen dürfen, bevor ein signifikanter Schaden entsteht. Das **Kritikalitätslevel** beschreibt den Zusammenhang zwischen Geschäftskritikalität und IT-System/Anwendung. Hat ein Ausfall eines Systems eine hohe Auswirkung auf das Unternehmen, dann ist das Kritikalitätslevel entsprechend hoch.
7	Zur **Operational Technologie (OT)** gehören Systeme zur Steuerung von industriellen Bereichen. Dazu zählen zum Beispiel Fertigungs- bzw. Produktionsanlagen oder computergesteuerte Lager.
7.3	Beim **Whitelisting** werden nur Verbindungen durchgelassen, deren Absender auf einer White-List stehen. Alle anderen Verbindungen werden blockiert.