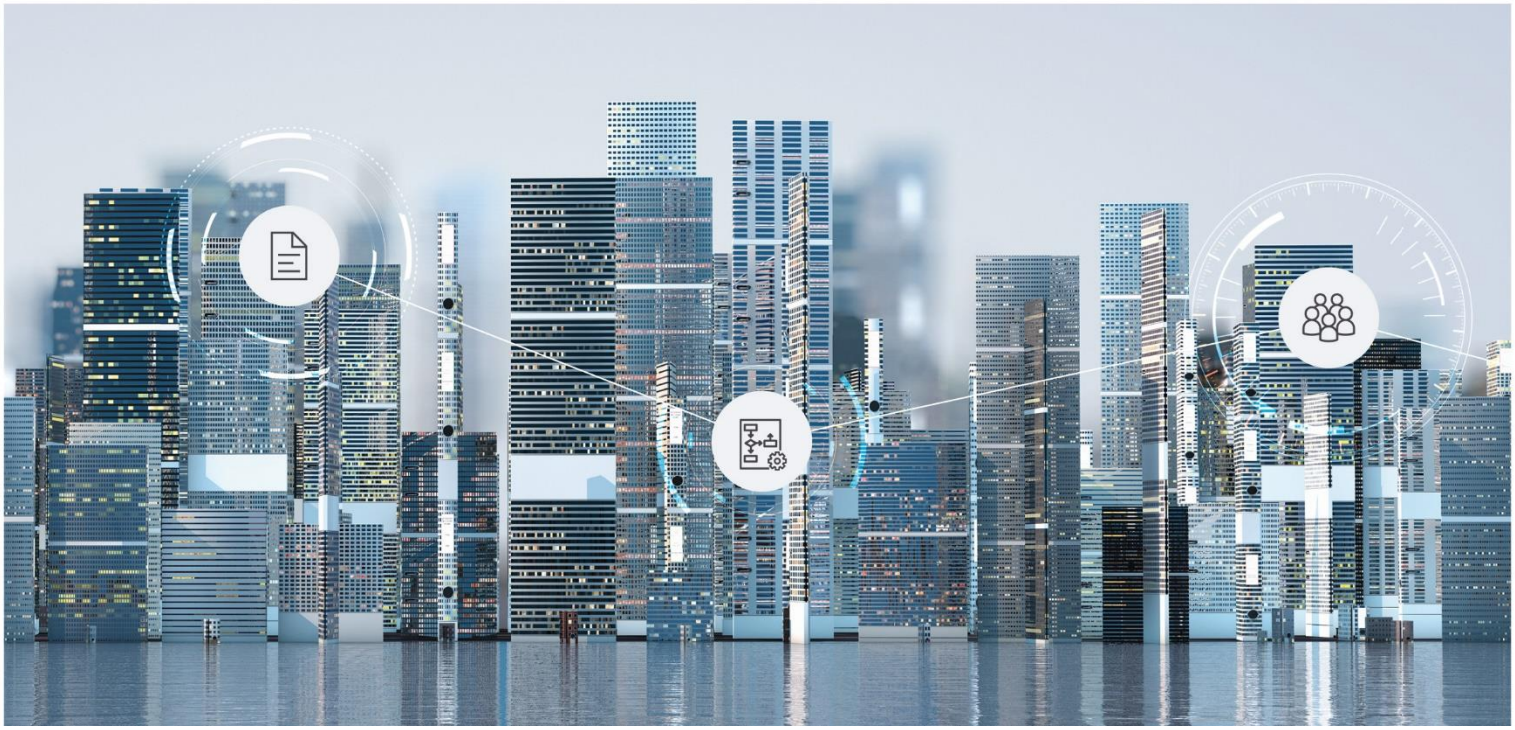

Technische und organisatorische Maßnahmen

Fabasoft Gruppe

Gültig ab 15.12.2022
Öffentlich

Die Weitergabe, Veröffentlichung und Vervielfältigung ist nicht gestattet.

Copyright © Fabasoft R&D GmbH, AT-4020 Linz, 2022.

Alle Rechte vorbehalten. Alle verwendeten Hard- und Softwarenamen sind Handelsnamen und/oder Marken der jeweiligen Hersteller.

Diese Unterlagen sind öffentlich.
Durch die Übermittlung und Präsentation dieser Unterlagen alleine werden keine Rechte an unserer Software, an unseren Dienstleistungen und Dienstleistungsresultaten oder sonstigen geschützten Rechten begründet.

Die Weitergabe, Veröffentlichung oder Vervielfältigung ist nicht gestattet.

Aus Gründen der einfacheren Lesbarkeit wird auf die geschlechtsspezifische Differenzierung, z. B. Benutzer/-innen, verzichtet. Entsprechende Begriffe gelten im Sinne der Gleichbehandlung grundsätzlich für beide Geschlechter.

Einleitung

Das vorliegende Dokument beschreibt die wesentlichen technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten im Rahmen der Geschäftstätigkeit der Fabasoft Gruppe (Fabasoft AG und ihre europäischen verbundenen Unternehmen, in der Folge „Fabasoft“).

Fabasoft verarbeitet personenbezogene Daten in einer Art und Weise, welche die Erreichung folgender Informationssicherheitsziele gemäß der Fabasoft Leitlinie zur Informationssicherheit sicherstellt:

Vertraulichkeit

Kundendaten, Geschäftsdaten und Daten der Entwicklungsbereiche unterliegen höchsten Vertraulichkeitsanforderungen. Sie dürfen nicht unrechtmäßig zur Kenntnis gelangen (limitierte Zugriffsberechtigungen, Vertraulichkeitsstufen, Verschlüsselung, ...). Informationen dürfen nur von autorisierten Personen eingesehen werden. Alle Fabasoft Mitarbeiter:innen sind zur Wahrung des anwendbaren Datengeheimnisses und zur Wahrung der Vertraulichkeit verpflichtet.

Integrität

Daten und Informationen müssen richtig und vollständig sein. IT-Systeme müssen durchgängig funktionieren. Daten und Informationen dürfen ohne Genehmigung nicht verändert werden. Veränderungen von Informationen müssen eindeutig erkennbar und nachvollziehbar sein (Versionierung).

Verfügbarkeit

Informationen müssen entsprechend der vertraglich zugesicherten Service Levels verfügbar sein. Ausfallzeiten dürfen keine wesentlichen Auswirkungen auf Fabasoft und ihre Stakeholder haben. Informationen müssen auf Systemen und Diensten verarbeitet werden, die notwendige Verfügbarkeit gewährleisten. Systeme und Dienste müssen im Störungsfall in der vereinbarten Zeit wiederhergestellt werden können.

Authentizität

Es muss gewährleistest werden, dass Informationen echt, überprüfbar und glaubwürdig sind und es sich um manipulationsfreie IT-Systeme und IT-Anwendungen handelt.

Technische und organisatorische Maßnahmen

In den folgenden Abschnitten werden die aktuellen technischen und organisatorischen Maßnahmen von Fabasoft beschrieben, die zur Erreichung der Sicherheitsziele implementiert wurden. Diese technischen und organisatorischen Maßnahmen werden regelmäßig auf ihre Aktualität, Wirksamkeit und Stand der Technik geprüft und gegebenenfalls präzisiert.

1 Vertraulichkeit

1.1 Zutrittskontrolle

Folgende Maßnahmen werden ergriffen, um Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen die personenbezogenen Daten verarbeitet werden, zu verwehren:

- Die Regelungen zur Sicherung physischen Zutritts sind in der Access Control Policy dokumentiert. Diese beinhaltet Regelungen hinsichtlich der physischen Sicherheit im Zusammenhang mit dem Gebäude und der Büroräumlichkeiten sowie die einhergehenden Überwachungsmaßnahmen.
- Fabasoft Räumlichkeiten werden in Sicherheitsstufen unterteilt. Mitarbeiter:innen erhalten nach den Kriterien der Access Control Policy die entsprechenden Zutrittsrechte.
- Fabasoft hat Verfahren implementiert, sodass Änderungen der Berechtigungen nur mit Genehmigung und in Übereinstimmung mit den Vorgaben und Richtlinien durchgeführt werden (Change Management).
- Fabasoft Mitarbeiter:innen erhalten einen Mitarbeiter:innenausweis, welcher an allen Fabasoft Standorten sichtbar zu tragen ist.
- Besucher:innen werden beaufsichtigt und von Mitarbeiter:innen begleitet. Externe Parteien, welche sich in definierten Räumlichkeiten aufgrund einer Genehmigung bewegen dürfen, sind zur Vertraulichkeit verpflichtet und müssen Ihre An- und Abmeldung im Fabasoft Office bekannt geben.

Folgende zusätzliche Maßnahmen werden für Rechenzentren ergriffen:

- Die Regelung zur Sicherung physischen Zutritts zu den Rechenzentren der Fabasoft sind im Dokument „Leistungsmerkmale Rechenzentrumsbetrieb Fabasoft Cloud“, abrufbar unter https://www.fabasoft.com/contract, festgehalten.
- Für alle Rechenzentren gelten strenge Sicherheitsmaßnahmen. Die externen Rechenzentren müssen den in der Checkliste für Standortprüfungen definierten Anforderungen (z.B. physische Sicherheit, Stromanbindung, Kühlung, Brandschutz, Netzwerkanbindung, Sicherheit, Umweltgefährdung, Aufrechterhaltung der Versorgungseinrichtungen, Betriebsredundanz, Schutz der Stromversorgung und Telekommunikationsleitungen) und organisatorischen Maßnahmen (z.B. Audits, Zertifizierungen) entsprechen.
- Ein technisches System überwacht kontinuierlich den Status der Racktüren, der Temperatur und der Stromversorgung und eskaliert bei Überschreitung des zulässigen Kontrollbereichs an das Incident Management.

1.2 Zugangskontrolle

Folgende Maßnahmen werden ergriffen, sodass eine Benützung von Datenverarbeitungssystemen durch Unbefugte verhindert wird:

- Der interne und externe Zugang auf das Fabasoft Netzwerk ist technisch stark eingeschränkt. Der externe Zugang auf das Fabasoft Netzwerk und die Anmeldung an Fabasoft Arbeitsplätzen ist mit einer Multi-Faktor-Authentifizierung implementiert.
- Die Regelungen zur Sicherung von Zugriffen auf Fabasoft Systeme und Dienste sind in der Access Control Policy dokumentiert. Diese beinhaltet Regelungen hinsichtlich der Vergabe, Ändern und Entzug von Berechtigungen auf Fabasoft Systemen und Dienste.

- Fabasoft hat Verfahren implementiert, sodass Änderungen der Berechtigungen nur mit Genehmigung und in Übereinstimmung mit den Vorgaben und Richtlinien durchgeführt werden (Change Management).
- Die Fabasoft Passwortrichtlinie legt die Anforderung zur Generierung, Änderung und Verwendung von Passwörtern fest.
- Die Zugangskontrolle wird mit dem Schutz der betroffenen Systeme durch folgende Maßnahmen unterstützt: Firewalls, Programme zur Erkennung von Schadsoftware, Einsatz von SIEM, laufendes Patch Management und Vulnerability Management.
- Nicht mehr benötigte vertrauliche Dokumente und Ausdrucke werden in den dafür vorgesehenen, geschlossenen Behältern (geschlossene Container mit Einwurföffnung) entsorgt. Die Container werden von einem externen Dienstleister regelmäßig abgeholt und der Container-Inhalt wird gemäß ÖNORM S 2109-1 Vernichtungsstufe 3 vernichtet.

1.3 Zugriffskontrolle

Nachstehende Maßnahmen werden ergriffen, damit Personen, die zur Nutzung von Datenverarbeitungssystemen berechtigt sind, nur Zugriff auf jene personenbezogenen Daten erhalten, für die sie Zugriffsrechte besitzen. Dadurch wird sichergestellt, dass personenbezogene Daten bei der Verarbeitung nicht unbefugt gelesen, kopiert, verändert oder gelöscht werden.

- Den Zugriff auf personenbezogene, vertrauliche oder sonstige sensible Informationen erhalten nur jene Personen, die zu diesem Zugriff durch ihre Leistungserbringung befugt werden („Least-Privileg-Model“/“Need-to-know-Prinzip“). Dabei werden auch die in der internen Klassifizierungs-Richtlinie definierten Vertraulichkeitsstufen berücksichtigt.
- Fabasoft definiert Verfahren und Anforderungen für die Protokollierung in Anwendungen und Diensten, den Schutz von Protokollen, die Aufbewahrung von Protokollen und die Verwendung von Protokolldaten.
- Fabasoft definiert Verfahren und Anforderungen für die Verschlüsselung von Daten bei der Übertragung (z. B. Protokolle, Chiffren) und im Ruhezustand (einschließlich Wechselmedien, Sicherungsdaten) sowie für die Schlüsselverwaltung (Schlüsselgenerierung, Ausstellung und Erhalt von Zertifikaten für öffentliche Schlüssel, Schlüsselschutz, Schlüsselwechsel, Umgang mit kompromittierten Schlüsseln, Rücknahme).

1.4 Trennungskontrolle

Folgende Maßnahmen werden ergriffen, damit personenbezogene Daten, die für unterschiedliche Zwecke erfasst werden, getrennt verarbeitet werden können:

- Die Trennung der Daten in den Produktionssystemen wird durch entsprechende Berechtigungen bzw. Mandantenmechanismen sichergestellt.
- Systeme für die Softwareentwicklung, Test- und Demosysteme sowie Produktionssysteme werden getrennt voneinander betrieben. Der Betrieb von Entwicklungs-, Test- und Produktionsumgebungen erfolgt auf getrennter Hardware bzw. virtuellen Maschinen.
- Systeme sind netzwerkseitig in adäquate Subnetze separiert.
- Über Firewall-Konfigurationen wird erreicht, dass die Kommunikation nur zwischen Netzsegmenten ermöglicht wird, für die die Kommunikation generell möglich sein muss.

- Es sind Anforderungen an die Konzeption von physischen und virtuellen Netzwerken, die Segmentierung und Isolierung (z. B. dedizierte Netzwerke für die Infrastrukturverwaltung) sowie den Schutz des Netzwerkperimeters definiert.

2 Integrität

2.1 Weitergabekontrolle

Folgende Maßnahmen werden ergriffen um zu verhindern, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transportes nicht unbefugt gelesen, verändert oder gelöscht werden können:

- Der Arbeitsvertrag regelt die Folgen von Verstößen gegen die Geheimhaltungs- und Vertraulichkeitspflicht. Auf das Fortbestehen der Geheimhaltungspflicht nach Beendigung des Arbeitsverhältnisses wird ausdrücklich hingewiesen. Jede/r Mitarbeiter:in erkennt diese Regelung durch seine Unterschrift als verbindlich an.
- Die Vereinbarung zur Informationssicherheit enthält für alle Fabasoft Mitarbeiter:innen Informationen hinsichtlich des sicheren Umgangs mit Daten und die zu verwendenden Systeme bei der Weitergabe von Daten.
- Verfahren und Anforderungen für die Verschlüsselung von Daten bei der Übertragung (z. B. Protokolle, Chiffren) und im Ruhezustand (einschließlich Wechselmedien, Sicherungsdaten) sowie für die Schlüsselverwaltung (Schlüsselgenerierung, Ausstellung und Erhalt von Zertifikaten für öffentliche Schlüssel, Schlüsselschutz, Schlüsselwechsel, Umgang mit kompromittierten Schlüsseln, Rücknahme).

2.2 Eingabekontrolle

Folgende Maßnahmen werden ergriffen, damit eine nachträgliche Prüfung und Feststellung erfolgen kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind:

- Die Protokollierungs- und Überwachungsrichtlinie definiert Verfahren und Anforderungen für die Protokollierung in Anwendungen und Diensten, den Schutz von Protokollen, die Aufbewahrung von Protokollen und die Verwendung von Protokolldaten. Einzelne Produkte (beispielsweise Fabasoft Cloud) bieten die Funktionalität "Audit Logging" an und haben diese entsprechend umgesetzt. Dadurch kann überprüft und festgestellt werden, von wem personenbezogene Daten eingegeben oder verändert wurden.

2.3 Datenintegritätskontrolle

Folgende Maßnahmen werden ergriffen, damit unbefugte oder versehentliche Änderungen von personenbezogenen Daten verhindert werden:

- Fabasoft hat in der System Security Policy Schutzanforderungen für die Malware- und Virenschutzkonfiguration dokumentiert und diese umgesetzt.
- Schwachstellen, die für Fabasoft relevant sind, müssen vollständig adressiert werden und der Prozess des Schwachstellenmanagements muss geeignet, angemessen und effektiv sein.
- Die Time Synchronization Policy ist Voraussetzung für Zeitsynchronisierung.

- Der interne und externe Zugang auf das Fabasoft Netzwerk ist technisch stark eingeschränkt. Der externe Zugang auf das Fabasoft Netzwerk und die Anmeldung an Fabasoft Arbeitsplätzen ist mit einer Multi-Faktor-Authentifizierung implementiert.

3 Verfügbarkeit

3.1 Verfügbarkeitskontrolle

Folgende Maßnahmen werden ergriffen, um personenbezogene Daten vor versehentlicher oder nicht autorisierter Vernichtung oder Verlust zu schützen:

- Es sind Verfahren zur Sicherung und Wiederherstellung von Systemen dokumentiert.
- Die Verfügbarkeit der Systeme wird laufend durch Systeme überwacht und eskaliert bei Abweichungen an das Incident Management.
- Es wird jährlich ein mögliches Notfallszenario entworfen und das Vorgehen in diesem Szenario im Rahmen einer Notfallübung getestet.
- Der Business Continuity Management Prozess ist so gestaltet, dass auf Sicherheitsereignisse, die den Geschäftsbetrieb stören, reagiert, diese gemildert und wiederhergestellt werden können. Die Notfallreaktion muss alle Prozesse des Notfallmanagements regeln, die darauf abzielen, die Auswirkungen und Folgen von Schäden so gering wie möglich zu halten.
- Notfälle werden regelmäßig getestet. Der Test muss die Anforderungen des Verfügbarkeitsmanagements und die Verfügbarkeit von Schlüsselpersonal berücksichtigen. Fabasoft testet und übt regelmäßig Notfälle auf Basis einer Risikobewertung.

3.2 Belastbarkeit und Wiederherstellbarkeit der eingesetzten IT-Systeme

Folgende Maßnahmen werden ergriffen, um Vorsorge zu treffen, damit eingesetzte Systeme und Dienste im Störungsfall in der notwendigen Zeit wiederhergestellt werden können:

- Die Fabasoft SaaS/Cloud Services werden regelmäßig Sicherheitsaudits oder Penetrationstests unterzogen, bei denen Schwachstellen, Sicherheitsmängel oder Probleme bei der Isolation/Segregation von Teamräumen festgestellt werden.
- Bei Sicherheitsaudits oder Penetrationstests festgestellte Schwachstellen, Sicherheitsmängel oder Probleme bei der Isolierung/Segregation von Teamräumen werden behoben.
- Fabasoft hat Verfahren zur Sicherung und Wiederherstellung von Systemen in der Fabasoft SaaS/Cloud-Umgebung im Leitfaden Backup and Recovery Operations dokumentiert.

Folgende zusätzliche Maßnahmen werden für Rechenzentren ergriffen:

- Fabasoft betreibt Komponenten für Fabasoft SaaS/Cloud Services, Mindbreeze InSpire SaaS und Fabasoft interne Services in externen Rechenzentren. Die externen Rechenzentren müssen definierten Anforderungen (z.B. physische Sicherheit, Stromanbindung, Kühlung, Brandschutz, Netzwerkanbindung, Sicherheit, Umweltgefährdung, Aufrechterhaltung der Versorgungseinrichtungen, Betriebsredundanz, Schutz der Stromversorgung und Telekommunikationsleitungen) und organisatorischen Maßnahmen (z.B. Audits, Zertifizierungen) entsprechen.
- Fabasoft SaaS/Cloud Daten (Metadaten und Dokumente) werden in geografisch verteilten Rechenzentren gespeichert.

4 Authentizität

Folgende Maßnahmen werden ergriffen, um Nutzer bei Zugriff auf personenbezogene Daten zu identifizieren und zu authentifizieren:

- Fabasoft hat Vorgaben in Richtlinien definiert, welche Passwort- und Vertraulichkeitsanforderungen für die Identifizierung und Authentifizierung beim Zugriff auf Fabasoft-interne Informationsbestände vorgeben.
- Die Authentifizierung in der Fabasoft Cloud erfolgt auf Basis einer MFA.

5 Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen

5.1 Auftragskontrolle

Folgende Maßnahmen werden ergriffen, damit personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden:

- Die Purchasing Policy hat bei Beauftragung von sicherheitsrelevanten Lieferanten und Dienstleistern Vorgaben (z.B. Kommunikation von Schwachstellen, Sicherheitsvorfällen oder Störungen) für alle Bestellungen bei Fabasoft-Lieferanten und Dienstleistern zu definieren, die wesentliche Teile zur Entwicklung oder zum Betrieb der Fabasoft Services beitragen und sich im Rahmen ihrer Geschäftsbeziehung durch bestimmte in der Policy definierte Merkmale auszeichnen.
- Lieferanten bzw. Dienstleister sind zur Einhaltung der Einkaufsbedingungen (einschließlich Geheimhaltungsverpflichtungen, Auftragsverarbeitungsvereinbarungen und damit einhergehende Bestimmungen) verpflichtet.
- Die Auftragsverarbeitungsvereinbarungen sowie die „Leistungsmerkmale Datensicherheit Fabasoft Cloud“ als Teil des „Cloud-Service-Agreements Fabasoft Cloud“ werden auf die Einhaltung der EU Cloud CoC-Kriterien überprüft.
- Alle Verarbeitungstätigkeiten werden in einem Verarbeitungsverzeichnis festgehalten. Die Verfahren umfassen die Art personenbezogener Daten sowie die damit verbundenen Prozesse, Systeme und Dritte, die an der Verarbeitung dieser Daten beteiligt sind.

5.2 Datenschutzmanagement

Folgende Maßnahmen werden ergriffen, um datenschutzrechtliche Anforderungen zu planen, umzusetzen, zu steuern und zu kontrollieren:

- Die Fabasoft Gruppe verfügt über ein Datenschutzteam ("Privacy Team"), das mit datenschutzrechtlichen Fragen und der Einhaltung der Anforderungen der DSGVO betraut ist. Fabasoft hat externe Datenschutzbeauftragte bestellt.
- Die Fabasoft Privacy Policy definiert und kommuniziert Grundsätze, die als datenschutzrechtliche Gebote zu verstehen sind, die in allen Bereichen der Geschäftstätigkeit von Fabasoft zu beachten sind, zB die Einhaltung von Privacy by Design und Privacy by Default-Prinzipien nach Art 25 DSGVO.
- Fabasoft hat den Prozess "Bearbeitung von Anfragen durch das Privacy Team" in einer Prozessbeschreibung dokumentiert. Die Prozessbeschreibung berücksichtigt neben den einschlägigen rechtlichen Anforderungen insbesondere die Einhaltung des EU Cloud Code of Conduct.

- Die Vereinbarung zur Informationssicherheit enthält für alle Fabasoft Mitarbeiter:innen Informationen über alle Kommunikationskanäle, die für Anfragen und Berichte bezüglich Sicherheit, Datenschutz und Compliance zu verwenden sind.
- Alle Verarbeitungstätigkeiten werden in einem Verfahrensverzeichnis festgehalten und regelmäßig aktualisiert.
- Konzernweit wurde eine Plattform implementiert, bei der regelmäßige Kurse zur Informationssicherheit und zum Datenschutz von allen Mitarbeiter:innen absolviert werden, um das Sicherheitswissen und -bewusstsein zu verbessern und den Mitarbeiter:innen ein angemessenes Sicherheitsverhalten vorzuleben.

5.3 Security Incident Management

Folgende Maßnahmen werden ergriffen, um sicherheitsrelevante Vorkommnisse zu erkennen, zu steuern zu überwachen und zu kontrollieren:

- Sicherheitsrelevante Vorkommnisse werden im Rahmen des Security Incident Management bewertet.
- Die Auswirkungen von Sicherheitsereignissen werden analysiert, kategorisiert/klassifiziert, gemäß Security Incident Management Prozess priorisiert und gegebenenfalls als Sicherheitsvorfall bearbeitet.
- Der Security Incident Management Prozess beinhaltet konkrete Vorgaben zur Reaktion (CSIRT und Kommunikationsstruktur, Analyse des Sicherheitsvorfalls einschließlich betroffener Systeme und Daten, Beweissicherung, Risikobewertung, Informationspflichten, Eindämmung, Schadensbegrenzung, Beendigung der Bedrohung und Wiederherstellung des Betriebs).