



WHITEPAPER INKLUSIVE SELF-ASSESSMENT

IT-Resilienz

Wie hoch ist die Widerstandsfähigkeit
Ihrer IT-Organisation?



Inhalt

Alte Gewohnheiten und neue Trends.....	02
Umfassende Risikobetrachtung.....	03
Resilienz: Kein Zufallsprodukt.....	03
IT-Resilienz – ein interdisziplinärer Ansatz.....	04
Self-Assessment IT-Resilienz.....	05
Softwaregestützte Management- systeme als Mittel der Wahl.....	19
Über DextraData.....	20

Zunehmende Digitalisierung und wachsende Vernetzung verdeutlichen: Geschäftsprozesse sind ohne den Einsatz von IT kaum noch denkbar. Durch die starke Involvement der IT werden die Herausforderungen für Unternehmen und ihre IT-Organisationen komplexer denn je: der Schutz von Know-how, von Daten und Geschäftsprozessen muss gewährleistet sein. Egal ob Großkonzern oder Mittelstandsunternehmen – über alle Branchen hinweg nimmt die Gefährdungslage zu.

Alte Gewohnheiten und neue Trends

Die Missachtung von altbekannten sowie neuen IT-Risiken – insbesondere in Krisenzeiten – gefährdet den ökonomischen Erfolg und Fortbestand des Unternehmens. Faktoren, die das Gefährdungspotenzial maximieren, sind neue Angriffsmethoden wie Ransomware-Attacken. Altbekannte Techniken wie Phishing werden von Angreifern weiter verfeinert. Zeitgleich vergrößerte sich die Bandbreite der Angriffsvektoren. Allerdings nicht allein, wie man vermuten mag, durch ungesicherte Netzwerke oder Internet-of-Things-Geräte: Problematischer sind der Trend der Verlagerung von Anwendungen in die Cloud und die gestiegene Verbreitung von Software-as-a-Service-Modellen. Denn beide Trends geben Daten in hohem Umfang in die Hände eines Dienstleisters. Die Sicherheitslücken Ihres Dienstleisters sind somit auch die Schwachstellen Ihres Unternehmens.

Noch wahrscheinlicher ist es, dass ein Datenleck durch den Faktor Mensch ermöglicht wird. Mitarbeiter- und Systemzugangsdaten sind ein begehrtes Ziel von Hackerangriffen. Daher ist die Sensibilisierung der eigenen Mitarbeiter für die Methoden von Cyber-Kriminellen von immenser Bedeutung. Alte Gewohnheiten, wie dasselbe Passwort für alle Online-Dienste, müssen einem verantwortungsvollen, sicherheitsorientierten Handeln im Arbeitsalltag weichen. Ein systematisches Vorgehen unterstützt dabei: IT-Sicherheit lässt sich dort organisatorisch verbessern, wo ein Informationssicherheits-Management-System (ISMS) und die darin hinterlegten Prozesse und Verantwortlichkeiten implementiert bzw. angepasst wurden. Die Chancen der Digitalisierung lassen sich nur dann ausschöpfen, wenn Sie die mit ihr verbundenen Risiken beherrschen.



» Auf Unternehmensebene heruntergebrochen, steht Resilienz für die Fähigkeit eines Unternehmens oder einer Organisationseinheit nach einer Störung wieder arbeitsfähig zu sein. «

Umfassende Risikoerfassung

Deutlich wird: Erfolg und Fortbestand von Unternehmen sind eng damit verbunden, wie das Unternehmen mit Risiken umgeht. Sie sind dazu verpflichtet Risiken entsprechend zu managen und die eigenen Funktionen kurzfristig wiederherzustellen. In diesem Kontext spricht man von der Selbstregulation und einer Steuerung der eingetretenen Risiken. Diese lassen sich minimieren, reduzieren, mit einer Versicherung transferieren oder gar akzeptieren. Eine möglichst vollständige Erfassung von Risiken ist die Voraussetzung für abzuleitende Maßnahmen.

Zur vollständigen Erfassung eines Risikos gehören seine Eintrittswahrscheinlichkeit und letztlich seine Auswirkung. Diese Betrachtungsweise der Auswirkung im Falle eines Risikoereignisses kann um eine weitere Ebene ergänzt werden: die der Überwindung von Schadensereignissen.

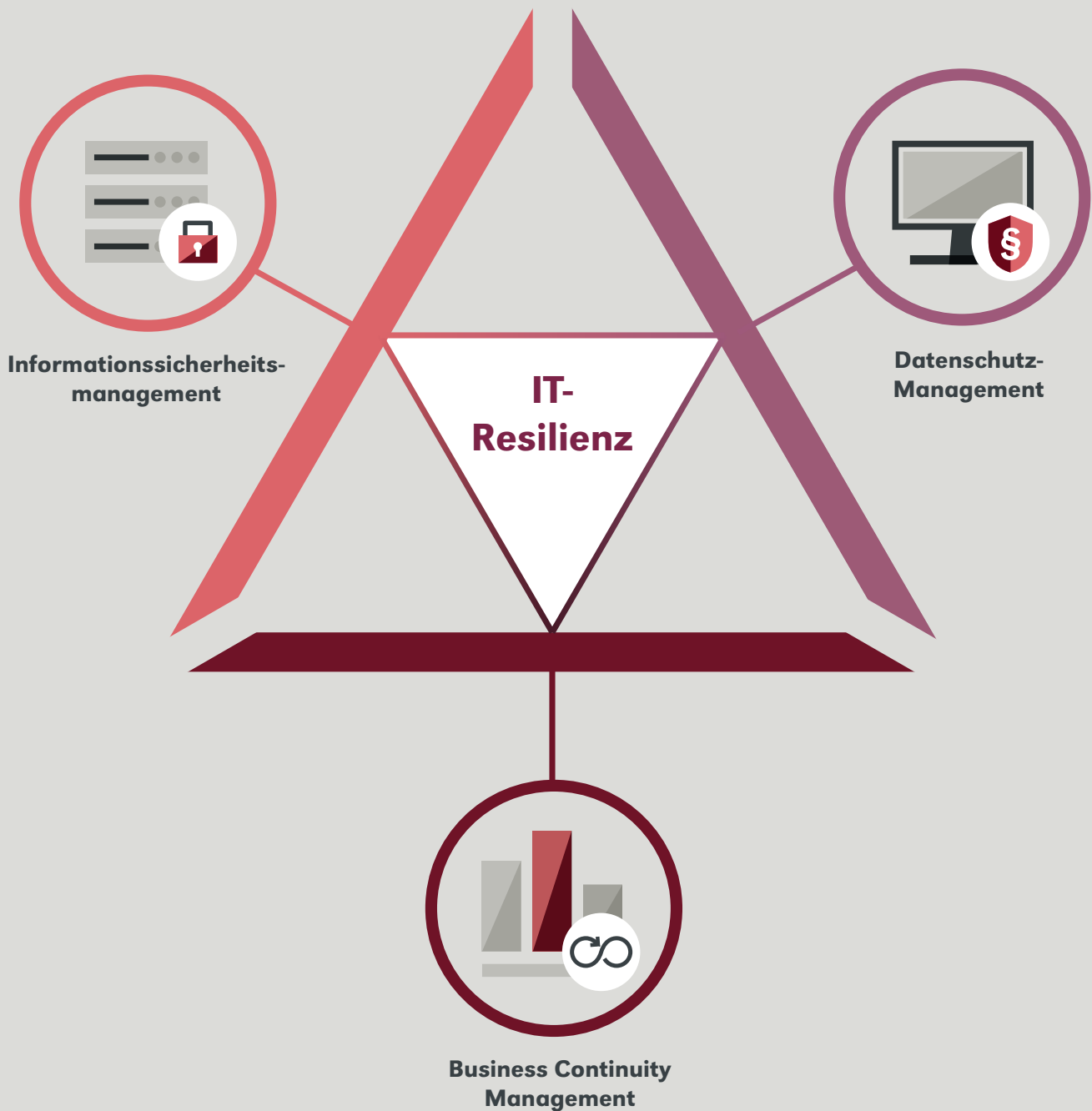
Resilienz: Kein Zufallsprodukt

Auf der Makro-Ebene gilt die Resilienz als Indikator dafür, ob und wie Gesellschaften kritische Situationen technologisch, sozial und wirtschaftlich souverän meistern. Auf Unternehmensebene heruntergebrochen, steht Resilienz für die Fähigkeit eines Unternehmens oder einer Organisationseinheit nach einer Störung wieder arbeitsfähig zu sein. Solche Organisationen zeichnen sich dadurch aus, dass sie über Kapazitätsreserven verfügen und flexibel genug sind, ihre Fähigkeiten an neue Bedingungen anzupassen.

Zum Aufbau und Ausbau der Resilienzfähigkeit sollten Organisationen:

- bewusst Redundanzen anlegen,
- über breit gestreute Ressourcen verfügen,
- sich selbst organisieren können,
- auch mit unvorhergesehenen Ereignissen rechnen,
- sich auf die eigenen Fähigkeiten und Stärken fokussieren
- und dazu fähig sein, ihre Prozesse zu flexibilisieren.

Konzerne mit gewachsenen Strukturen tendieren dazu, im Normalfall nicht benötigte Strukturen aus Kostengründen abzubauen. Auch kleine und mittlere Unternehmen möchten von der Philosophie des Lean Thinking profitieren. Denn auch sie verschlanken Strukturen, um Kosten zu reduzieren. Resilienz ist jedoch kein Zufallsprodukt, denn gänzlich ohne zusätzliche Kosten und Ressourcen lässt sie sich nicht aufbauen. Ein Kernkonflikt jeder Organisation, die krisensicher aufgestellt sein möchte, bildet daher die Balance zwischen Effizienz und Resilienz.



IT-Resilienz – ein interdisziplinärer Ansatz

Wie lässt sich IT-Resilienz – sprich die Widerstandsfähigkeit eines IT-Systems oder einer IT-Organisation – ermitteln? In dem Sie herausfinden, wie performant das System oder die Organisation während einer größeren Unterbrechung oder Krise weiter funktioniert. Im Best-Case mit möglichst minimalen Auswirkungsgrad auf Geschäfts- und Betriebsprozesse. Denn die verbundenen Risiken für die Geschäftskontinuität können sich beispielsweise in Produktivitätsminderungen, unterbrochenen Lieferketten oder verschobenen Kundenkontaktpunkten manifestieren.

Die Aufrechterhaltung der IT bei Störungen oder (Teil-)Ausfällen, um Services oder Produkte weiterhin auf einem akzeptablen Niveau anbieten zu können, kann als Resultat des Business Continuity Managements (BCM) gewertet werden. Dabei handelt es sich um einen ganzheitlichen Prozess. Er identifiziert Risiken für die Prozesse und Ressourcen einer Organisation und analysiert ihre Auswirkungen im Eintrittsfall. Durch die Entwicklung entsprechender risikominimierender Maßnahmen soll die organisatorische Resilienz erhöht werden. ►

Diese Erhöhung führt zu einer effektiven, effizienten und vor allem angemessenen Prävention, Detektion und Reaktion auf Störungen. Noch tiefgreifender geht das IT-Notfallmanagement (bei ITIL auch IT Service Continuity Management genannt) vor.

Reicht Business Continuity Management als einzig praktizierte Disziplin aus, um IT-Risiken vollumfassend zu berücksichtigen? Die internationale Norm ISO/IEC 27001 für Informationssicherheit enthält unter anderem das Referenzmaßnahmenziel Informationssicherheitsaspekte beim Business Continuity Management. Sie formuliert darin Maßnahmen zur Aufrechterhaltung der Informationssicherheit.

Auch andere umgesetzte Maßnahmen der Informationssicherheit und des Datenschutzes können beispielsweise die Auswirkungen einer Ransomware-Attacke mit drohendem Verlust von Daten, definitiv ein Worst-Case-Szenario, abmil-

dern: Indem z. B. ein Account nur auf, für die Erfüllung einer Tätigkeit notwendige, statt auf alle verfügbaren Systeme und Daten zugreifen kann. Zusätzlich sollte dem Datenverlust mit zuverlässigen Backup-Funktionen entgegengewirkt werden. Letzteres fordert auch die EU-Datenschutzgrundverordnung (EU-DSGVO). Sie regelt durch geeignete Maßnahmen der Datensicherung den Schutz personenbezogener Daten.

Nach und nach wird klar: Eine geeignete Lösung kann darin bestehen, die Kontinuität des Geschäftsbetriebes um die Sichtweise der Gefahrenabwehr zu erweitern. Der interdisziplinär interpretierte Ansatz der IT-Resilienz wird damit Geschäftsprozessen gerecht, die ohne Einbeziehung der IT mittlerweile undenkbar wären. Der hier vorgestellte interdisziplinäre Ansatz berücksichtigt die Disziplinen Informationssicherheitsmanagement, Datenschutzmanagement und Business Continuity Management.

Self-Assessment IT-Resilienz

Inwieweit Auswirkungen abgemildert oder gar vermieden werden können, hängt vom spezifischen Szenario und den Maßnahmenzielen ab. Unser Self-Assessment verfolgt den vorab erläuterten interdisziplinären Ansatz. Es behandelt ausgewählte Fachfragen aus den Disziplinen Informationssicherheitsmanagement, Datenschutzmanagement und Business Continuity Management. Diese Fachfragen beinhalten wiederum ausformulierte, praxisbezogene Handlungsanweisungen und beziehen sich auf die Standards ISO/IEC 27001 und ISO 2301 sowie auf die Datenschutzgrundverordnung der Europäischen Union. Die vier Fragestellungen pro Disziplin bilden nur einen Teil des Weges zur IT-Resilienz ab. Sie sollen Ihnen ein grundlegendes Gespür für den Themenkomplex sowie erste Anhaltspunkte zur Umsetzung von geeigneten Maßnahmen vermitteln.





Registrierung und Deregistrierung von Benutzern

Haben Sie einen formalen Prozess für die Registrierung und Deregistrierung von Benutzern umgesetzt, um die Zuordnung von Zugangsrechten zu ermöglichen?

**NICHT
ERFÜLLT**

- Sie haben keinen formalen Prozess für die Registrierung und Deregistrierung von Benutzern umgesetzt, um die Zuordnung von Zugangsrechten zu ermöglichen.

ERFÜLLT

TEILWEISE ERFÜLLT

- Sie haben die Verwendung eindeutiger Benutzerkennungen, damit Benutzer mit deren Handlungen in Verbindung gebracht und verantwortlich gemacht werden können.
- Sie haben die Verwendung gemeinsam genutzter Kennungen nur gestattet, wenn dies aus geschäftlichen oder betrieblichen Gründen erforderlich ist. Zudem ist die Verwendung genehmigt und wird dokumentiert.
- Sie veranlassen die sofortige Deaktivierung oder Löschung der Kennungen von Benutzern, die die Organisation verlassen haben.
- Sie identifizieren, löschen und deaktivieren regelmäßig überflüssiger Benutzerkennungen als Prüfprozess.
- Die Gewährung bzw. der Entzug des Zugangs zu Informationen oder Einrichtungen zur Informationsverarbeitung erfolgt im Rahmen eines zweistufigen Verfahrens:
 1. Die Zuweisung und Aktivierung bzw. Entziehung einer Benutzerkennung
 2. Die Gewährung bzw. Entziehung der Zugangsrechte zu dieser Benutzerkennung

VOLL UMFÄNGLICH ERFÜLLT



Verwaltung privilegierter Zugangsrechte

Haben Sie die Zuteilung und den Gebrauch privilegierter Zugangsrechte eingeschränkt und gesteuert?

**NICHT
ERFÜLLT**

- Sie haben die Zuteilung und den Gebrauch privilegierter Zugangsrechte nicht eingeschränkt und nicht gesteuert.

ERFÜLLT

TEILWEISE ERFÜLLT

- Sie kontrollieren die Zuteilung von privilegierten Zugangsrechten durch einen offiziellen Genehmigungsprozess entsprechend der jeweiligen Zugangssteuerungsrichtlinie.
- Sie identifizieren die privilegierten Zugangsrechte, mit denen einzelne Systemen oder Prozessen verbunden sind, z. B. Betriebssystem, Datenbankverwaltungssystem und jede Anwendung sowie die Benutzer, denen sie zugewiesen werden sollen.
- Sie erteilen privilegierte Zugangsrechte Benutzern nur im Bedarfsfall und ereignisbezogen entsprechend der Zugangssteuerungsrichtlinie, d. h. auf Grundlage der Mindestanforderungen für deren Funktionsbereiche.
- Es existiert ein Genehmigungsprozess und eine aktuelle Aufstellung aller gewährten privilegierten Zugangsrechte. Privilegierte Zugangsrechte werden nicht vor Abschluss des Genehmigungsprozesses gewährt.
- Es sind Anforderungen bezüglich des Auslaufens von privilegierten Zugangsrechten festgelegt.
- Privilegierte Zugangsrechte werden einer anderen als der Benutzererkennung zugewiesen, die für die normalen Geschäftsaktivitäten verwendet wird. Normale Geschäftsaktivitäten werden nicht mit Benutzerkennungen ausgeführt, die über privilegierte Zugangsrechte verfügen.
- Die Kompetenzen von Benutzern mit privilegierten Zugangsrechten werden regelmäßig überprüft, um sicherzustellen, dass sie deren Aufgabenprofil entsprechen.
- Sie haben spezifische Verfahren eingerichtet und angewendet, mit denen eine unbefugte Nutzung von Benutzerkennungen mit allgemeinen Administratorrechten entsprechend den Konfigurationsmöglichkeiten des Systems verhindert wird.
- Bei Benutzerkennungen mit allgemeinen Administratorrechten wird die Vertraulichkeit der geheimen Authentifizierungsdaten bei einer gemeinsamen Nutzung gewahrt. Beispielsweise ändern Sie Kennwörter häufig sowie schnellstmöglich nach Ausscheiden oder Versetzung eines Benutzers mit privilegierten Zugangsrechten.

VOLL UMFÄHGLICH ERFÜLLT



Trennung von Entwicklungs-, Test- und Betriebsumgebungen

Haben Sie Entwicklungs-, Test- und Betriebsumgebungen voneinander getrennt, um das Risiko unbefugter Zugriffe auf oder Änderungen an der Betriebsumgebung zu verringern?

**NICHT
ERFÜLLT**

- Sie haben die Entwicklungs-, Test- und Betriebsumgebungen nicht voneinander getrennt, um das Risiko unbefugter Zugriffe auf oder Änderungen an der Betriebsumgebung zu verringern.

ERFÜLLT

TEILWEISE ERFÜLLT

- Sie haben festgestellt, wie stark Betriebs-, Test- und Entwicklungsumgebungen zur Verhinderung von Problemen im Betriebsablauf voneinander getrennt werden müssen und setzen die Trennung um.
- Sie haben Regeln für den Transfer von Software vom Entwicklungs- zum Betriebsstatus festgelegt und dokumentiert.
- Sie haben Entwicklungs- und Betriebssoftware auf unterschiedlichen Systemen oder Computerprozessoren und in unterschiedlichen Domänen oder Verzeichnissen laufen.
- Sie testen Änderungen an betrieblichen Systemen und Anwendungen vor der Anwendung auf die betrieblichen Systeme in einer Prüf- oder Staging-Umgebung.
- Nur in Ausnahmefällen führen Sie die Tests auf betrieblichen Systemen durch.
- Nur wenn es erforderlich ist, ist der Zugriff aus den betrieblichen Systemen auf Compiler, Editoren und andere Entwicklungswerkzeuge möglich.
- Sie verwenden für die betrieblichen und die Testsysteme unterschiedliche Benutzerprofile, die in den Menüs entsprechend angezeigt werden, um das Risiko eines Fehlers zu verringern.
- Sie kopieren sensible Daten nicht in das System der Testumgebung, ohne Maßnahmen für das Testsystem zur Verfügung zu haben.

VOLL UMFÄNGLICH ERFÜLLT



Handhabung von technischen Schwachstellen

Haben Sie Information über technische Schwachstellen verwendeter Informationssysteme rechtzeitig eingeholt, die Gefährdung der Organisation durch derartige Schwachstellen bewertet und angemessene Maßnahmen ergriffen?

NICHT ERFÜLLT

- Sie haben keine Information über technische Schwachstellen verwendeter Informationssysteme rechtzeitig eingeholt, die Gefährdung der Organisation durch derartige Schwachstellen nicht bewertet und angemessene Maßnahmen nicht ergriffen.

ERFÜLLT

TEILWEISE ERFÜLLT

- Sie holen Informationen über technische Schwachstellen verwendeter Informationssysteme rechtzeitig ein. Zudem bewerten Sie die Gefährdung der Organisation durch derartige Schwachstellen und ergreifen angemessene Maßnahmen, um das dazugehörige Risiko zu behandeln.
 - Sie haben eine aktuelle und vollständige Aufstellung der Werte, um eine wirksame Handhabung technischer Schwachstellen zu ermöglichen. Inhaltlich haben Sie Software-Anbieter, Versionsnummern, den aktuellen Verteilungsstand (z. B. die Angabe, welche Software auf welchen Systemen installiert ist) und die für die Software innerhalb der Organisation zuständigen Personen. Als Reaktion auf die Feststellung potenzieller technischer Schwachstellen ergreifen Sie zeitnah angemessene Abhilfemaßnahmen. Dafür haben Sie einen effektiven Managementprozesses initiiert.
 - Sie haben in Ihrer Organisation zur Handhabung technischer Schwachstellen verbundenen Aufgaben und Verantwortlichkeiten festgelegt und eingerichtet. Somit können Sie die Überwachung auf Schwachstellen, die Risikobeurteilung von Schwachstellen, das Einspielen von Patches, die Nachverfolgung von Assets und sämtliche erforderlichen Koordinationsaufgaben sicherstellen.
 - Sie haben Informationsressourcen, die zur Feststellung relevanter technischer Schwachstellen und deren nachhaltiger Bewusstmachung verwendet werden hinsichtlich Software und anderer Technologien identifiziert. Diese Informationsressourcen werden bei Änderungen im Inventar oder bei Ermittlung neuer oder weiterer nützlicher Ressourcen aktualisiert.
-
- Sie haben einen Zeitplan zur Reaktion auf Benachrichtigungen über möglicherweise relevante technische Schwachstellen festgelegt.
 - Sie haben bei der Feststellung einer potenziellen technischen Schwachstelle einen Prozess initiiert, der innerhalb Ihrer Organisation die damit verbundenen Risiken feststellt und die erforderlichen Abhilfemaßnahmen bestimmt und spielen beispielsweise die erforderlichen Patches auf.
 - Sie haben einen Prozess in Ihrem Unternehmen initiiert, der je nach Dringlichkeit der Behebung einer technischen Schwachstelle die entsprechende Maßnahme nach den für die Änderungssteuerung geltenden Sicherheitsmaßnahmen berücksichtigt. Hierbei kommen auch Abhilfemaßnahmen bei Informationssicherheitsvorfällen in Frage. ►



Handhabung von technischen Schwachstellen

Haben Sie Information über technische Schwachstellen verwendeter Informationssysteme rechtzeitig eingeholt, die Gefährdung der Organisation durch derartige Schwachstellen bewertet und angemessene Maßnahmen ergriffen?

- Sie können bewerten, ob der Patch aus einer vertrauenswürdigen Quelle zur Verfügung steht und können die damit verbundenen Risiken bewerten.
- Sie testen und beurteilen die Patches vor der Installation, um sicherzustellen, dass diese keine inakzeptablen Auswirkungen auf den Regelbetrieb hervorrufen.
- Sie haben einen Prozess in Ihrer Organisation initiiert, falls kein Patch zur Verfügung steht, um andere Maßnahmen zu ergreifen. Beispielsweise die Abschaltung der Dienste bzw. Funktionen, welche von der Schwachstelle betroffen sind oder eine Anpassung bzw. Ergänzung der Zugriffssteuerung, z. B. Firewalls, an den Netzwerkgrenzen. In Frage kommt auch verstärkte Überwachung zur Erkennung stattfindender Angriffe oder eine Sensibilisierung der Beschäftigten für die Schwachstelle.
- Sie haben alle durchgeführten Verfahren in einem Audit-Protokoll vermerkt.
- Sie überwachen und bewerten regelmäßig den Prozess zur Handhabung technischer Schwachstellen, um die Wirksamkeit und Effizienz sicherzustellen.
- Sie behandeln Hochrisikosysteme bevorzugt.
- Sie haben die Aktivitäten zur Handhabung technischer Schwachstellen mit den Aktivitäten zum Umgang mit Sicherheitsvorfällen abgestimmt. Somit werden Daten über Schwachstellen an die für Abhilfemaßnahmen zuständige Person weitergeleitet und es stehen bei einem Sicherheitsvorfall die durchzuführenden technischen Verfahren zur Verfügung.
- Sie haben ein Verfahren zum Umgang mit Situationen festgelegt, in denen eine Schwachstelle festgestellt wurde, aber keine geeignete Gegenmaßnahme existiert. Sie beurteilen in diesen Situationen die Risiken, die die bekannte Schwachstelle birgt, und legen geeignete Erkennungs- und Abhilfemaßnahmen fest.



Haben Sie einen Überblick, in welchen Applikationen personenbezogene Daten verarbeitet werden?

**NICHT
ERFÜLLT**

- Sie haben keinen Überblick, in welchen Applikationen personenbezogene Daten verarbeitet werden.

ERFÜLLT

TEILWEISE ERFÜLLT

- Sie haben eine aktuelle Übersicht aller in Ihrer Organisation vorhandenen Applikationen.
- Sie haben eine aktuelle Übersicht der jeweiligen Applikations-Owner.
- Sie haben eine vollständige Applikationsbeschreibung, die auch den Verarbeitungszweck der Software definiert.
- Sie haben eine Gewichtung der Applikation für die Verfügbarkeit der Kernprozesse im Unternehmenskontext vorgenommen.
- Sie haben die Datenkategorien definiert, um eine Einteilung besonders sensibler Informationen vornehmen zu können.

VOLL UMFÄSSLICH ERFÜLLT



Haben Sie einen Prozess für die Umsetzung der Löschung von personenbezogenen Daten in Ihren Applikationen initiiert?

**NICHT
ERFÜLLT**

- Sie haben keinen Prozess für die Umsetzung der Löschung von personenbezogenen Daten in Ihren Applikationen initiiert.

ERFÜLLT

TEILWEISE ERFÜLLT

- Sie haben für jede Applikation in Ihrem Unternehmen, welche personenbezogene Daten verarbeitet, ein Löschkonzept erstellt.
- Sie haben Angaben zu dem System, Hersteller und Funktion beschrieben. Zudem haben Sie die Datenkategorien und Datenarten definiert, die innerhalb des Systems verarbeitet werden.

- Sie haben den Datenfluss über die Schnittstellen vor- und nachgelagerter Systeme beschrieben.
- Sie haben einen Löschrmechanismus initiiert und die Löschrregeln definiert.

- Ihre Organisation ist jederzeit in der Lage, die Löschung der Daten nachweisen zu können. Den Nachweis realisieren Sie über Screenshots, Skripte, Systemeinsicht oder Logfiles.

VOLL UMFÄSSLICH ERFÜLLT



Haben Sie einen Prozess zur Beauskunftung der betroffenen Person nach Art. 15 EU-DSGVO in Ihrem Unternehmen initiiert?

**NICHT
ERFÜLLT**

- Sie haben keinen Prozess zur Beauskunftung der betroffenen Person nach Art. 15 EU-DSGVO in Ihrem Unternehmen initiiert.

VOLL UMFÄHGLICH ERFÜLLT

ERFÜLLT

TEILWEISE ERFÜLLT

- Sie haben einen Überblick, an welchen Stellen in Ihrem Unternehmen personenbezogene Daten verarbeitet werden.
 - Sie haben eine Lösung etabliert, um alle personenbezogenen Daten zu einer natürlichen Person zusammenzustellen. Die Lösung beinhaltet die Möglichkeit die Beauskunftung entsprechend der gesetzlichen vorgegebenen Frist umzusetzen.
 - Sie können den Zweck der Verarbeitung der personenbezogenen Daten beschreiben und der Zweck entspricht den gesetzlichen Vorgaben.
-
- Sie können die Datenkategorien beschreiben und den Datenfluss der personenbezogenen Daten beauskunften.
-
- Sie können die geplante Dauer der Verarbeitung der personenbezogenen Daten beschreiben und die Dauer entspricht den gesetzlichen Vorgaben.



Haben Sie angemessene technische Maßnahmen für die Applikationen umgesetzt?

**NICHT
ERFÜLLT**

- Sie haben keine angemessenen technischen Maßnahmen für Ihre Applikationen umgesetzt.

ERFÜLLT

TEILWEISE ERFÜLLT

- Sie haben in Ihrem Unternehmen eine Multi-Faktor-Authentifizierung für alle Benutzer aktiviert.
- Sie haben ein Konzept zur Verschlüsselung von kritischen Daten und Dokumenten verankert.
- Sie haben ein Backup mit Wiederherstellungsfunktion, welches für die Infrastruktur Ihres Unternehmens angemessen ist.
- Sie haben Maßnahmen etabliert, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.
- Sie haben über eine Eingabekontrolle eine Protokollierung erreicht, die auf verschiedenen Ebenen stattfindet. Sie haben definiert, welche Daten protokolliert werden und wer Zugriff auf Protokolle hat.

VOLL UMFÄNGLICH ERFÜLLT

Business Continuity Management



Haben Sie eine Policy für das BCM im Unternehmen festgelegt, die den BCM-Lifecycle nach den »BCI Good Practices« berücksichtigt?

**NICHT
ERFÜLLT**

- Sie haben eine Policy für das Unternehmen festgelegt, die den BCM-Lifecycle nach den »BCI Good Practices« nicht berücksichtigt.

VOLL UMFÄNGLICH ERFÜLLT

ERFÜLLT

TEILWEISE ERFÜLLT

- Sie erstellen im ersten Schritt des Lifecycles die BCM-Policy. Darin legen Sie den groben Rahmen für das BCM fest und haben ein geeignetes Dokument zur Kommunikation im Unternehmen. Nachdem die Policy abgestimmt und durch die Geschäftsführung gegengezeichnet ist, können Sie das BCM-Handbuch erstellen. Dieses Dokument konkretisiert das Vorgehen im BCM. Es beschreibt die Methoden und Regeln, die im BCM angewendet werden.
- Sie verankern das Thema BCM innerhalb der gesamten Organisationsstruktur. Dazu ist es wichtig, dass das BCM sich an den strategischen Unternehmenszielen ausrichtet. Sämtliche Interessengruppen im Unternehmen müssen ein einheitliches Verständnis vom Thema erlangen. Die Schaffung von Awareness und Akzeptanz kann beispielsweise durch ein auf das Unternehmen und dessen Mitarbeiter zugeschnittenes Schulungsprogramm und die offene Kommunikation erreicht werden. Schlussendlich müssen die Synergieeffekte mit anderen Management-Disziplinen erkannt und herausgestellt werden, damit BCM nicht als zusätzliche Last, sondern als nützliches Hilfsmittel verstanden wird.
- Im Anschluss an die Erstellung bzw. Aktualisierung der Policy und des Handbuchs findet die Analyse statt. Zunächst wird die Business Impact Analyse (BIA) durchgeführt, in der die zeitkritischen Geschäftsprozesse und die benötigten Ressourcen inklusive ihrer BC-Anforderungen identifiziert werden. Wurden diese identifiziert, wird die Risikoanalyse durchgeführt, in der mögliche Risiken, die zu einem Ausfall der Geschäftsprozesse führen könnten, bestimmt und bewertet werden.
- Sie identifizieren während der Designphase mögliche BC-Lösungsoptionen und Maßnahmen, die die Einhaltung der Anforderungen aus der Analysephase sicherstellen können und bestehende Risiken minimieren. Zudem werden die Optionen und Maßnahmen einer Kosten-Nutzen-Analyse unterzogen und der Geschäftsführung zur Auswahl vorgelegt. Anschließend können dann die Fachbereiche die, für sie passenden, Lösungen wählen.
- Sie beschreiben während der Implementierungsphase Pläne, wie die gewählten BC-Lösungen im Einzelfall konkret umzusetzen sind. Die Pläne beinhalten die notwendigen Ressourcen sowie die Notfallorganisation und Reaktionsstruktur.
- Die Policy und das komplette BCM unterliegen einem kontinuierlichen Verbesserungsprozess. Der Geltungsbereich wird mit der Zeit immer weiter gefasst, um eine möglichst vollumfängliche Absicherung der Organisation zu erzielen. Erkenntnisse aus Übungen und Tests finden hierbei eine Berücksichtigung und werden zur Überprüfung von Plänen und getroffenen Maßnahmen verwendet.

Business Continuity Management



Haben Sie innerhalb der BCM-Policy eine Abgrenzung für das IT-Service Continuity Management (ITSCM) vorgenommen?

**NICHT
ERFÜLLT**

- Sie haben innerhalb der BCM-Policy keine Abgrenzung zum ITSCM vorgenommen.

ERFÜLLT

TEILWEISE ERFÜLLT

- Sie haben ITSCM als eigene Managementdisziplin im Unternehmen verankert.
- Sie verweisen innerhalb der BCM Policy auf die mitgeltenden Dokumente des IT-Service Continuity Managements.

- Die Wiederanlaufparameter für das ITSCM beziehen sich auf die Analysephase des BCM inklusive der manuellen Überbrückungsphasen.

- Sie haben individuelle Wiederanlauf- und Wiederherstellungs-Pläne für ausgefallene IT-Komponenten in zeitkritischen Geschäftsprozessen erstellt.

VOLL UMFÄSSLICH ERFÜLLT

Business Continuity Management



Betrachten Sie alle Geschäftsprozesse, die zur Aufrechterhaltung der Geschäftstätigkeit erforderlich sind?

**NICHT
ERFÜLLT**

- Sie betrachten nicht alle Geschäftsprozesse, die zur Aufrechterhaltung der Geschäftstätigkeit erforderlich sind.

ERFÜLLT

**TEILWEISE
ERFÜLLT**

- Sie verfügen über eine komplette Prozesslandkarte.
- Sie betrachten alle Geschäftsprozesse, die zur Aufrechterhaltung der Geschäftstätigkeit erforderlich sind und verfügen über eine komplette Prozesslandkarte.
- Sie berücksichtigen priorisierte Prozesse sowie die dazu notwendigen Ressourcen und Prozessabhängigkeiten.

**VOLL UMFÄNGLICH
ERFÜLLT**

Business Continuity Management



Existiert ein Übungs- und Testkonzept und decken die Konzepte alle geplanten Ausfallszenarien ab?

NICHT
ERFÜLLT

- Es existiert kein Übungs- und Testkonzept.

ERFÜLLT

TEILWEISE
ERFÜLLT

- Sie verfügen über ein Übungs- und Testkonzept für ausgewählte Szenarien.
- Sie verfügen über ein Übungs- und Testkonzept für den Ausfall von Standort bzw. Gebäude.
- Sie verfügen über ein Übungs- und Testkonzept für den Ausfall von Personal.
- Sie verfügen über ein Übungs- und Testkonzept für den Ausfall von IT bzw. Infrastruktur.
- Sie verfügen über ein Übungs- und Testkonzept für den Ausfall von Dienstleistern und Zulieferern.
- Sie verfügen über ein Übungs- und Testkonzept für den Ausfall von Produktionsanlagen.
- Sie verfügen über ein Übungs- und Testkonzept für alle Szenarien sowie eines Volltestes.

VOLL UMFÄSSLICH
ERFÜLLT

Softwaregestützte Managementsysteme als Mittel der Wahl

Praktiker stehen vor der Herausforderung, Maßnahmen anhand strategischer und überlebensnotwendiger Ziele abzuleiten, die sich nur mit einem systematischen Ansatz priorisieren lassen. Managementsysteme können hier als Mittel der Wahl Abhilfe verschaffen, da sie Ressourcen bündeln und Abläufe effizienter machen. So lassen sich Anforderungen aus Normen, Gesetzen und Kundenwünschen systematisch gesteuert realisieren.

Baut eine Organisation sukzessive mehrere Managementsysteme auf, kann es unübersichtlich werden und zu Überschneidungen kommen. Abhilfe verschafft in diesem Falle ein integriertes Managementsystem. Die gleichbleibende Grundstruktur der unterschiedlichen ISO-Managementsystemnormen, die sogenannte High Level Structure (HLS), verringert durch gemeinsame Definitionen und identische Anforderungen die Komplexität.

Insbesondere softwaregestützte Managementsysteme, sprich der Einsatz einer Software zum Aufbau und Betrieb eines Managementsystems, steigern diesen Effizienzgewinn noch deutlicher. Das Management von Risiken, Audits, Feststellungen und Maßnahmen wird durch die Möglichkeiten der digitalen Dokumentation erleichtert. Idealerweise lassen sich die Grundzüge eines Managementsystems durch eine intuitive Bedienung und einen Zugewinn an Übersichtlichkeit noch leichter erlernen sowie erfassen. Ähnlich den Synergien, die sich aus dem gleichbleibenden Aufbau der HLS ergeben, werden Unternehmensstrukturen, Prozesse, Systeme und Applikationen in modernen Lösungen nur einmalig erfasst.

Digitalisierte Managementsysteme mit GRASP.

Erfassen Sie Ihre Risiken
effizient & anwenderfreundlich.

Mehr erfahren auf
dextradata.com/grasp



Über DextraData

Seit 1995 unterstützt DextraData Unternehmen bei der Planung und Realisierung von IT-Projekten bis hin zur Verantwortung für den Regelbetrieb. In den Themenbereichen Informationssicherheit, Business Continuity und Datenschutz verfügen wir über eine umfassende Consulting-Expertise und sind damit Partner für Unternehmen, die sich den aktuellen Herausforderungen der digitalen Transformation stellen.

Als Independent Software Vendor entwickelt DextraData innovative Software, die Transparenz schafft, Prozesse optimiert sowie Entscheidungshilfe und Mehrwerte für das Business liefert. Mit GRASP (Governance, Risk, Audit Software-Plattform) haben wir eine Lösung entwickelt, die es Organisationen ermöglicht die einst parallel und analog betriebene Managementsystem-Dokumentation einfach und schnell zu digitalisieren.

© Copyright 2021 DextraData

Autoren: N. Vorholt, B. Vorholt, D. Schröder,
F. Lukasik, B. Seum
Konzeption u. Realisierung: F. Lukasik
Lektorat: B. Seum
Layout: M. Gonska

KONTAKT

DextraData GmbH
Girardetstraße 4 • 45131 Essen
Telefon +49 201 9 59 75 0
info@dextradata.com • www.dextradata.com

DextraData

