
Democratizing
Information
Security
www.opexaadvisory.de
Opexa™
Advisory
Please hold the handrail
Please stand on the right

Opexa®
Advisory

Geschäftsrisiko Cybersicherheit:

Was ist ihr „Plan B“, wenn die Systeme ausfallen?

4.6.2024

Bildhinweis: Generiert mit MS Copiilot

Klaus Kilvinger

- Gründer & Geschäftsführender Gesellschafter der Opexa Advisory GmbH
- Informationssicherheitsmanager
- Besondere Expertise im Bereich der Informationssicherheit und in zertifizierten Managementsystemen (ISO 27001, TISAX®, B3S)
- CISO / ISB für verschiedene Unternehmen
- Sprecher zur Informationssicherheitsmanagement für Veranstaltungen der DGQ, IHK München/Oberbayern, IMH, Verband Öffentlicher Banken, BVMW, Management Circle
- Langjährige Expertise im Bereich IT- Serviceindustrie und Software-Qualitätssicherung mit umfangreicher Führungserfahrung

Metatrends / Regulatorik

Infosec Bedrohungen wachsen

Digitalisierung nimmt zu Anzahl der Attacken (Menge, Komplexität) wächst, es bedarf höherer Resilienz

NIS 2 – EU-Richtlinie

Erhöhung der Anforderungen zu Cybersicherheit in vielen Unternehmen (ca. 40.000 in DE)

- Termin 10/2024
- Unternehmen ab 50 MA / 10 Mio. € Umsatz
- Ausbau auf 18 Sektoren, u.a. Manufacturing (u. a. Medizingeräte, Forschung), Fahrzeugbau

EU-Maschinenrichtlinie NEU

- KI-Risiken sind zu berücksichtigen
- Cybersicherheit

Fachkräfte- und Wissensmangel

Wenige Fachleute, wenig Budget für Fortbildung, KMU besonders kritisch

DORA im Finanzbereich

Resilienzerhöhung dank EU-Richtlinie

- Infrastruktur, Prozesse, Cloud, IKT
- Gesamte Finanzbranche (> 1.000 in DE) betroffen

IEC 62443 Netzwerksicherheit

Operational Technology / Industrial Automation & Controls / Infrastruktur Manufacturing für Betreiber, Anbieter und Serviceorganisationen

Metatrends / Regulatorik

Infosec Bedrohungen wachsen

Digitalisierung nimmt zu Anzahl der Attacken (Menge, Komplexität) wächst, es bedarf höherer Resilienz

Fachkräfte- und Wissensmangel

Wenige Fachleute, wenig Budget für Fortbildung, KMU besonders kritisch

KI - Verordnung

Cyber Resilience Act

NIS 2 – EU-Richtlinie

Erhöhung der Anforderun
vielen Unternehmen (ca.

- Termin 10/2024
- Unternehmen ab 50 MA
- Ausbau auf 18 Sektoren, u.a. Manufacturing (u. a. Medizingeräte, Forschung), Fahrzeugbau

EU-Maschinenrichtlinie NEU

- KI-Risiken sind zu berücksichtigen
- Cybersicherheit

anzbereich

g dank EU-Richtlinie

rozesse, Cloud, IKT

nzbranche (> 1.000 in DE) betroffen

IEC 62443 Netzwerksicherheit

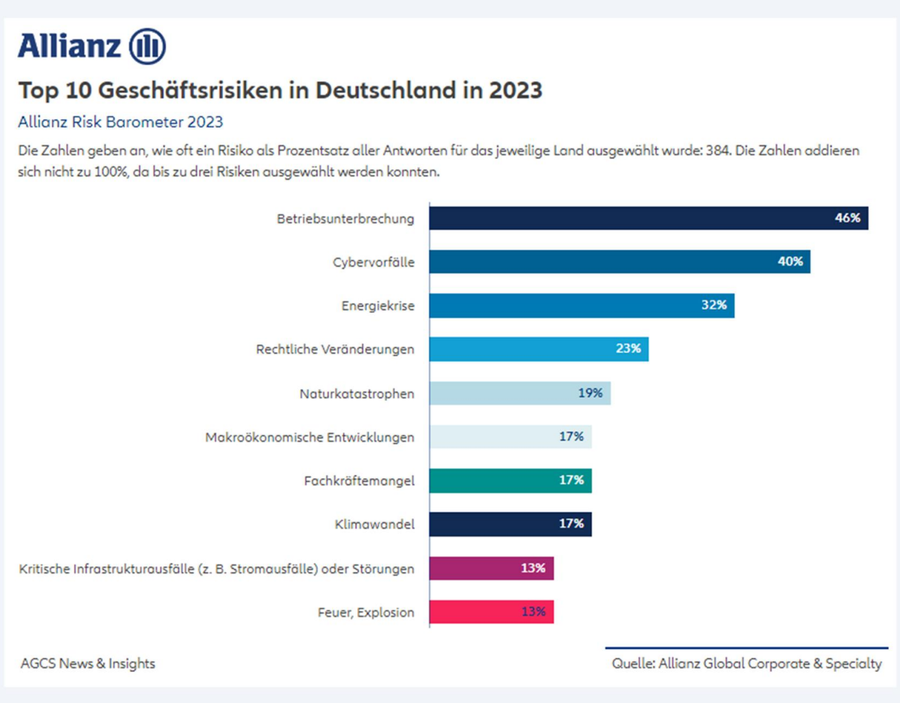
Operational Technology / Industrial Automation & Controls / Infrastruktur Manufacturing für Betreiber, Anbieter und Serviceorganisationen

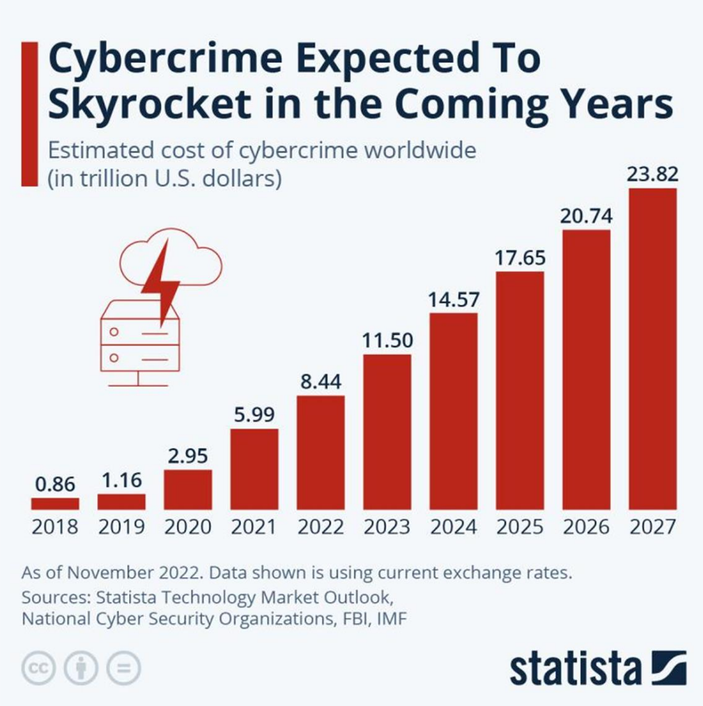
Irrtümer

- „Bei uns passiert schon nichts“
- „Wir sind zu klein und somit nicht interessant für Kriminelle“
- „Notfallmanagement mit Übungen ist zu viel Aufwand im Verhältnis zum Nutzen“

→ Sie fahren gewissermaßen mit einer „digitalen Seifenkiste“, die fährt, aber keine ausreichenden Bremsen und Schutzmaßnahmen für die Passagiere hat!

Fakten





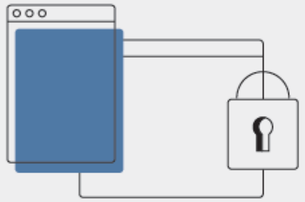
Gesamtschaden von 223 Milliarden Euro durch Diebstahl, Spionage und Sabotage. Die Schadenssumme ist mehr als doppelt so hoch wie in den Jahren 2018/2019.Bitkom. Neun von zehn Unternehmen (88 Prozent) waren 2020/2021 von Angriffen betroffen [1].

BSI: Im Jahr 2022 wurde im Durchschnitt **täglich mindestens ein** deutsches Unternehmen Ziel eines Ransomware-Angriffs

Ransomware

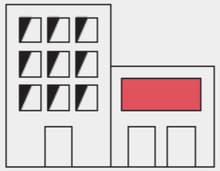
ist weiterhin die größte Bedrohung.

2 **Ransomware-Angriffe** auf Kommunalverwaltungen oder kommunale Betriebe wurden durchschnittlich pro Monat bekannt.



68 erfolgreiche **Ransomware-Angriffe auf Unternehmen** wurden bekannt.

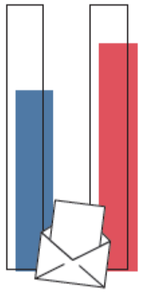
15 davon richteten sich gegen **IT-Dienstleister.**



Mehr als **2.000** **Schwachstellen** in Software-Produkten **(15 % davon kritisch)** wurden im Berichtszeitraum durchschnittlich im Monat bekannt. Das ist ein **Zuwachs von 24 %.**

Eine Viertelmillion
neue **Schadprogramm-Varianten** wurden durchschnittlich an jedem Tag im Berichtszeitraum gefunden.

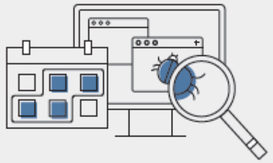
66%
aller **Spam-Mails** im Berichtszeitraum waren Cyberangriffe:
34% Erpressungsmails,
32% Betrugsmails



84%
aller betrügerischen E-Mails waren **Phishing-E-Mails** zur Erbeutung von Authentisierungsdaten, meist bei Banken und Sparkassen.

Top 3-Bedrohungen je Zielgruppe:

Gesellschaft	Wirtschaft	Staat und Verwaltung
		
Identitätsdiebstahl	***Ransomware***	***Ransomware***
Sextortion	Abhängigkeit innerhalb der IT-Supply-Chain	APT
Phishing	Schwachstellen, offene oder falsch konfigurierte Online-Server	Schwachstellen, offene oder falsch konfigurierte Online-Server



Rund **21.000** **infizierte Systeme** wurden täglich im Berichtszeitraum erkannt und vom BSI an die deutschen Provider gemeldet.

Durchschnittlich rund **775** **E-Mails mit Schadprogrammen** wurden an jedem Tag im Berichtszeitraum in deutschen Regierungsnetzen abgefangen.

370 **Webseiten** wurden im Durchschnitt an jedem Tag des Berichtszeitraums für den Zugriff aus den Regierungsnetzen gesperrt. **Der Grund:** Die Seiten enthielten Schadprogramme.

6.220 2022
5.100 2021

7.120 Teilnehmer hatte die **Allianz für Cyber-Sicherheit** im Jahr 2023.

Deutschland **Digital•Sicher•BSI•**

Fakten KMU

- Arbeitsschritte auch bei KMU werden zunehmend digitalisiert, was bei inkorrekter Nutzung und bei Nicht-Instandhaltung der Software zur erhöhten Angriffsfläche für potenzielle Angriffe aus dem Internet führt
- In Produktion oft noch alte Systeme ohne aktuelle Patchmöglichkeiten (Win NT, 95, 2000)
- Vielen kleinen und mittleren Unternehmen ist die Gefahr eines potenziellen Angriffs nicht bewusst
- KMU werden vermehrt Ziel von Cyberattacken
- Die meisten Angriffe erfolgen großflächig und automatisiert
- Unternehmen werden **nicht im Einzelnen als Ziel** ausgewählt
- Das Internet wird von Hackern unter anderem auf genutzte Software mit Sicherheitslücken gescannt, die sie ausnutzen können, um ein System mit Schadsoftware zu kompromittieren

Folgen eines Notfalls

Direkte Kosten/Folgen

- Produktionsausfall und Umsatzausfall (teilweise nicht kompensierbar)
- Logistik (Lagerung Teile, Transport. Lieferkette)
- Wiederanlaufkosten (Ausschuss, Maschinen)
- Bewältigungskosten (Forensik, Berater, Juristen usw.)
- Strafzahlungen wg. Terminverzug
- Bußgelder
- Auftragsverluste
- Leerzeiten/Kurzarbeit (Handhabung HR-Abteilung)
- Finanzlücke
- Insolvenz

Indirekte Kosten (Image etc.)

Notfallplan vorhanden?

- Laut einer Umfrage der IHK München aus 2023 haben **42 Prozent** der befragten bayerischen Unternehmen einen IT-Notfallplan
- Von den 42% ist aber nicht bekannt, ob er
  - **aktuell ist** (Namen, Rollen, Telefonnummern)
  - **geübt** wurde (Alle, Teams, Schreibtisch, Realität)
  - **erfolgreich** getestet wurde (Was ist Erfolg)
  - **gut und umfassend** ist (End-to-end)
  - **Varianten** hat (Ursachen)
  - **ausgedruckt** vorliegt (Nutzbar auch ohne IT)
  - **jährlich geprüft und fortgeschrieben** wird (QS, Aktualität, Stand der Technik)
- Umkehrschluss: **58% haben keinen Notfallplan**!

EY-Studie 2023 (Notfallmanagement)

Haben Sie einen Krisenplan für Fälle des Datendiebstahls?

13 % wissen nicht, ob sie einen haben, 17% haben keinen Plan.

Wie oft werden Abläufe geübt?

13% mehr als 1mal /Jahr, 45% 1mal/Jahr, 27% noch nie, 15 % nicht bekannt

Existiert ein zentrales Krisenteam?

56% nein, 11 % nicht bekannt, 33% ja

Wie wichtig ist die Kommunikation (intern/extern)?

50% wichtig, 37% bedingt wichtig, Rest „nicht wichtig“ oder „keine Angabe“

EY-Studie 2023 (Notfallmanagement)

Haben Sie einen Krisenplan für Fälle des Datendiebstahls?

13 % wi

Wie

13% m

Existi

56% nein, 11 % nicht bekannt, 33% ja

Munich Re - Umfrage: 87 % der befragten Manager gaben an, dass ihr Unternehmen nicht ausreichend gegen Cyber-Risiken geschützt ist.

Wie wichtig ist die Kommunikation (intern/extern)?

50% wichtig, 37% bedingt wichtig, Rest „nicht wichtig“ oder „keine Angabe“

Störung-Notfall-Krise

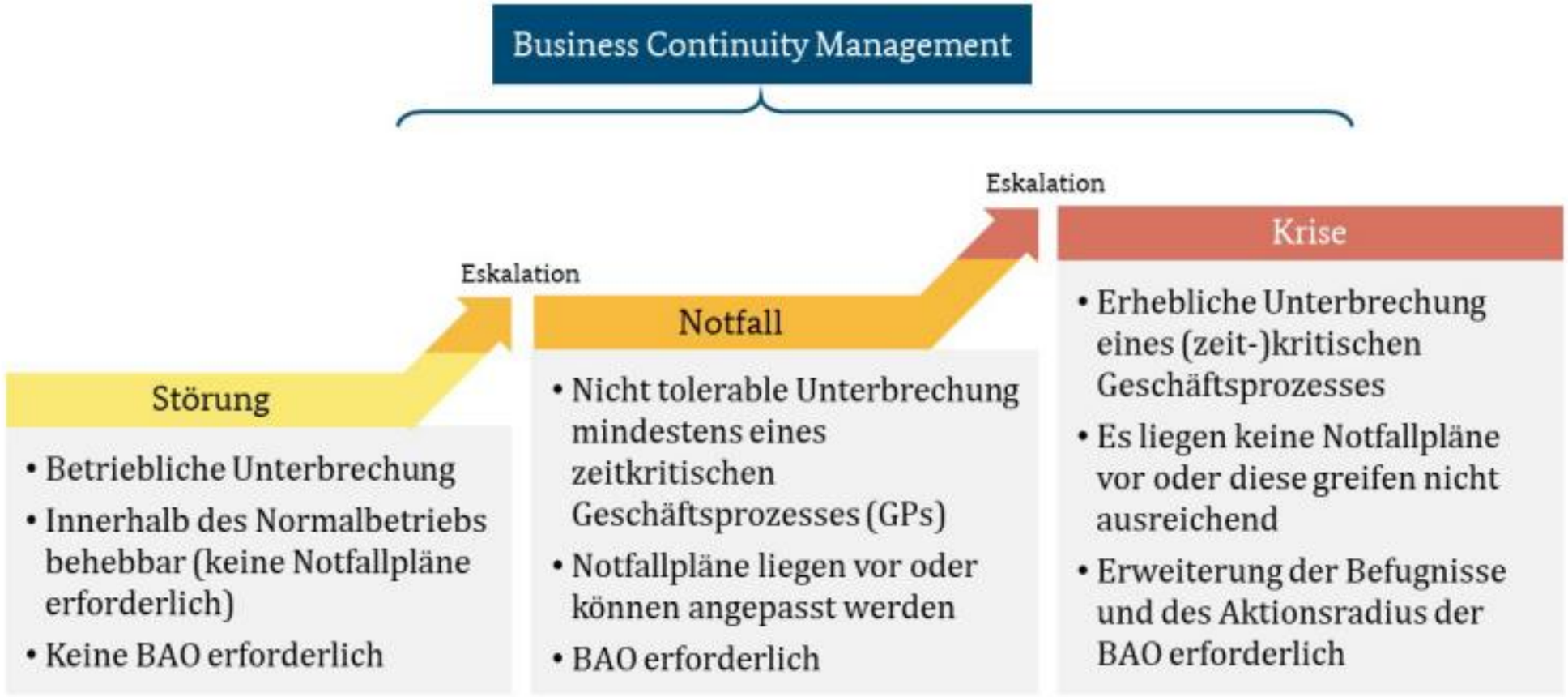


Abbildung 2: Abgrenzung Störung, Notfall, Krise

Quelle: BSI 200-4

Meldungen

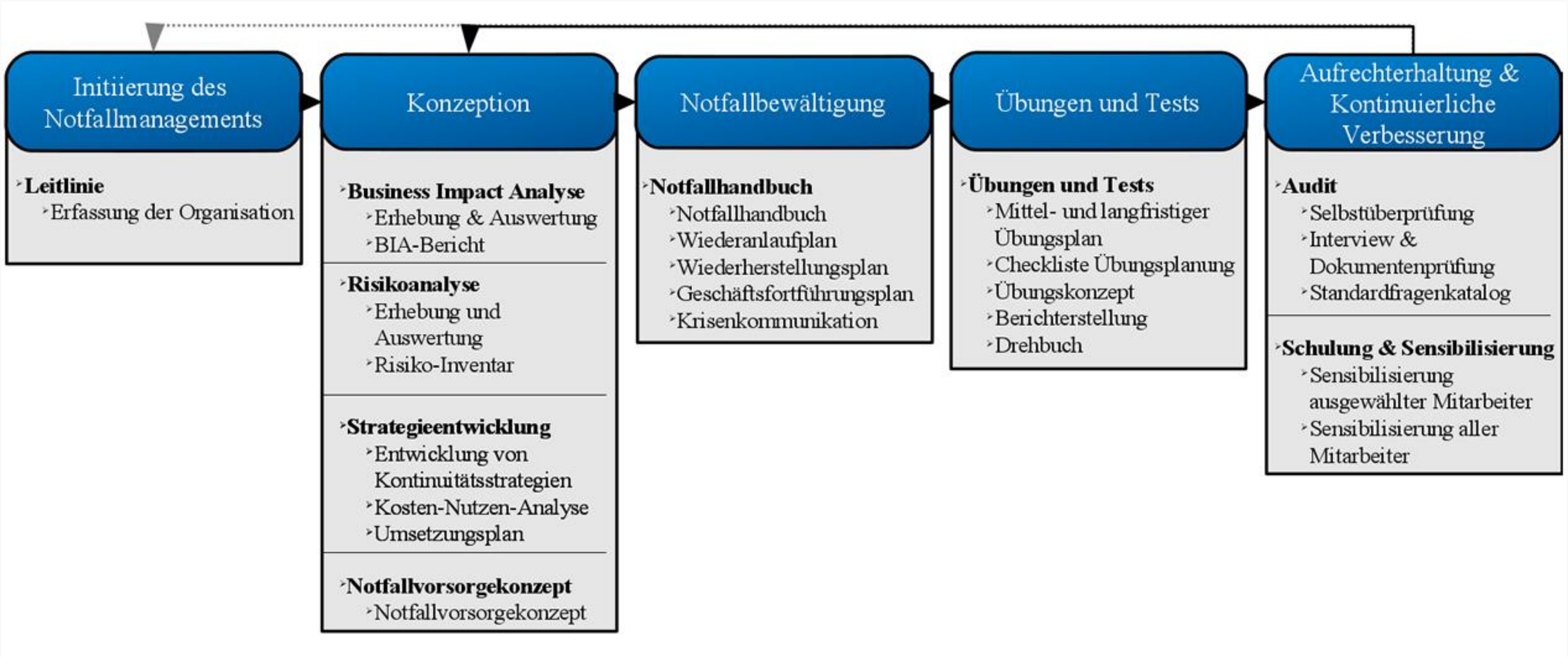
- Meldewege (Persönlich, Telefon, Mail, Papier, Intranet)
- Adressat (Geschäftsführung, Vorgesetzte, Werkschutz, Hotline)
- Inhalt (Was ist passiert, Wo ist es passiert, Wer ist betroffen, Was ist die Auswirkung, Wie bin ich für Rückfragen erreichbar)
- Zeitliche Komponente
- Gesetzlich vorgeschriebene Meldungen (DSGVO, Kritis, NIS-2)

→ Häufigste Probleme sind Unwissenheit, Unkenntnis Meldeweg und –kanal, Desinteresse, Faulheit, Angst vor der Meldung (Denunziantentum, Folgeaufwand, Ärger, Zeitverlust, Vorwürfe)

→ Awareness ist wichtig

→ Kultur und innere Einstellung zum Arbeitgeber

BSI 100-4 Umsetzungsrahmen



Quelle: BSI

BSI 100-4 Umsetzungsrahmen

Quelle: BSI

BSI 100-4 Reifegrad

Umsetzungsgrad III:

- Vollständige Bearbeitung aller Phasen des Notfallmanagements

Umsetzungsgrad II:

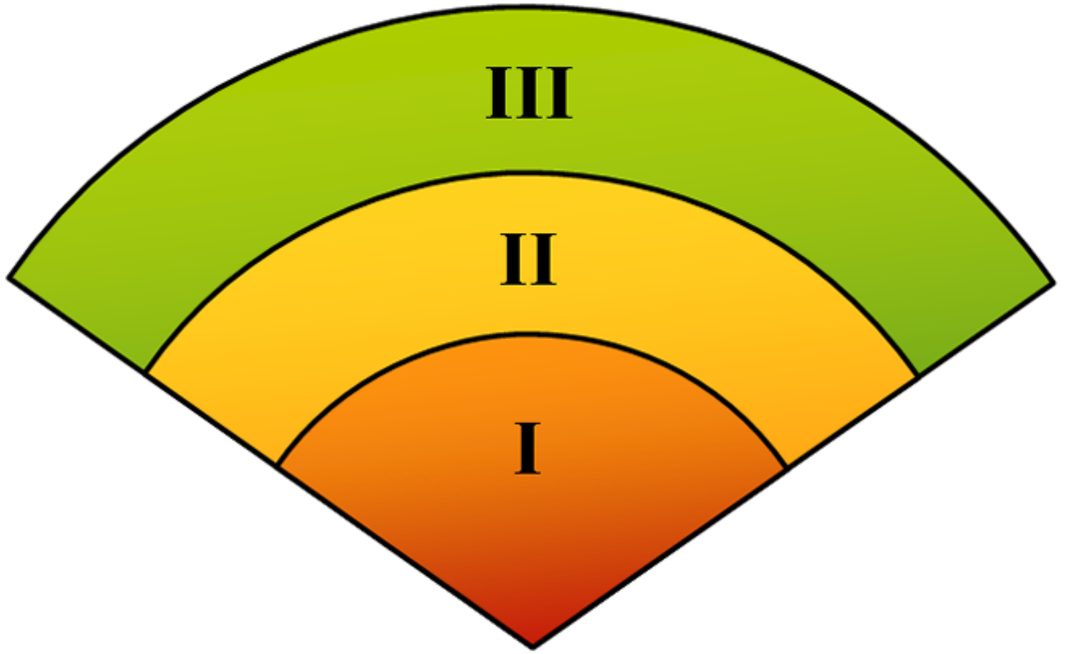
- Präventive und reaktive Notfall-reaktion definiert und beschrieben
- Übungen und Tests sowie kontinuierliche Weiterentwicklung in Grundsätzen beschrieben

Umsetzungsgrad I:

- Ermöglichung eines Notfallmanagements
- Teilweise ist die Notfallbewältigung möglich oder initial vorbereitet
- Prozesse sind nicht beschrieben

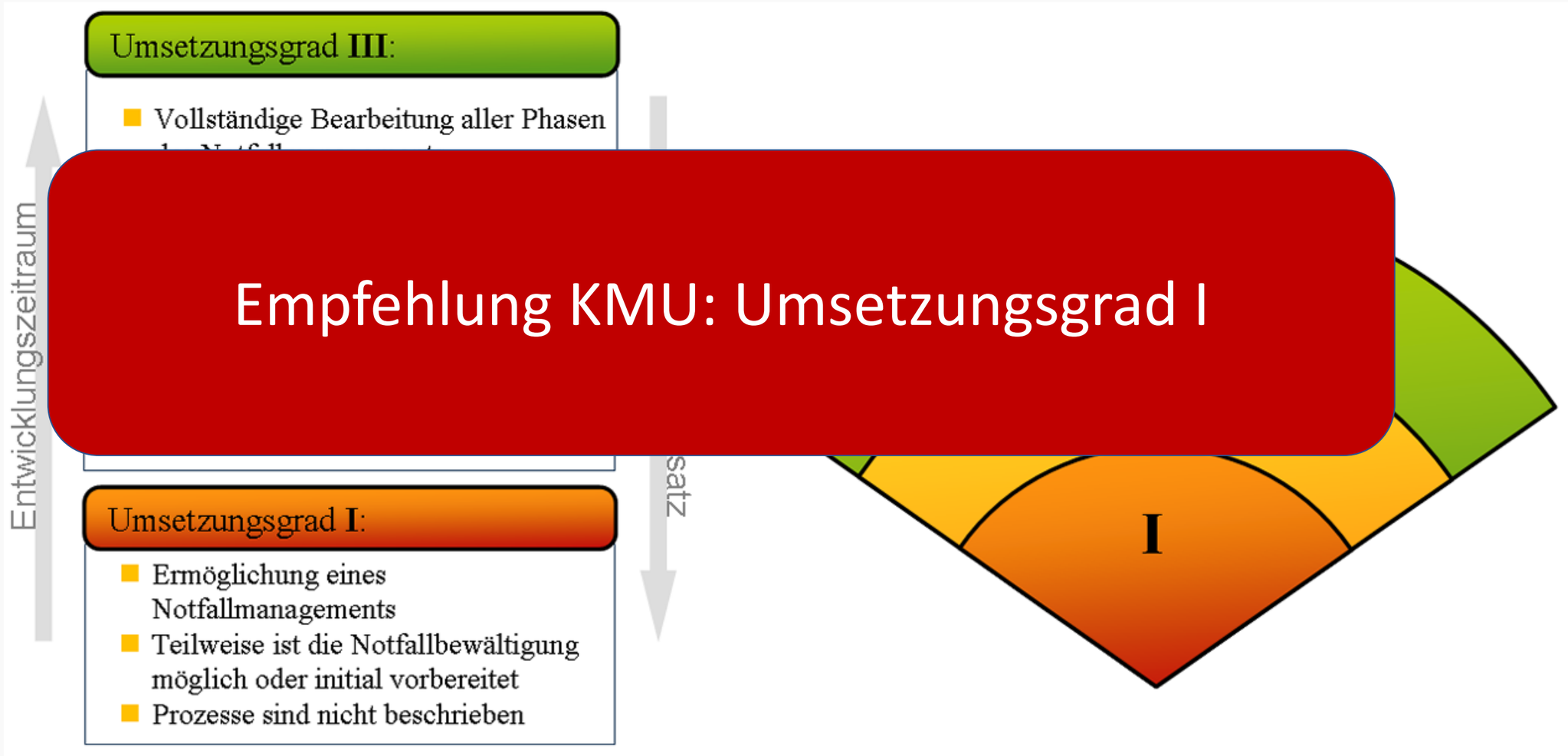
Entwicklungszeitraum

Ressourceneinsatz



Quelle: BSI

BSI 100-4 Reifegrad



Empfehlung KMU: Umsetzungsgrad I

Quelle: BSI

Normenkanon

- ISO 31000 Risikomanagement
- BSI 200-4, Business Continuity Management (erklärende Texte und konkrete Anforderungen)
- Anforderungskatalog zum BSI-Standard 200-4 (inkl. Mapping zu ISO 22301)
- Deutscher Corporate Governance Codex
- ISO 22301 Business Continuity Management (zertifizierbar) legt die **Anforderungen an die Implementierung**, **Aufrechterhaltung** und **Verbesserung** eines Managementsystems fest, um sich vor Störungen zu **schützen**, die **Wahrscheinlichkeit** des Auftretens von Störungen zu **verringern**, sich darauf vorzubereiten, darauf zu **reagieren** und sich von ihnen zu **erholen**, wenn sie auftreten.

ISO/IEC 27001 & BSI

27001 Normtext

- Rollen und Verantwortlichkeiten sind festzulegen (Wer wird im Notfall involviert, Verantwortlich)
- Risikobasiertes Vorgehen
- Risikoassessments und deren Behandlung
- Performanceevaluationen, Audits, PDCA

27001 Anhang

- Control: 5.7 Threat Intelligence (Sammlung von Informationen zu möglichen Bedrohungen)
- Control 5.26 Response to information security incidents (Reaktionen nach Plan)
- Control 5.30 ICT Readiness for business continuity
- Control 6.3 Information security awareness, education and training
- Control 8.13 Information Backup

BSI 200-4

Anforderungskatalog zum BSI-Standard 200-4 gibt einen komprimierten Überblick zu allen MUSS- und SOLLTE-Anforderungen des Standard-BCMS.

DIN SPEC 27076

Organisation, Kenntnisse und Management für Notfälle sind Teil der Analyse

ISO/IEC 27001 & BSI

27001 Normtext

- Rollen und Verantwortlichkeiten sind festzulegen (Wer wird im Notfall involviert, Verantwortlich)
- Risikobasiertes Vorgehen
- Risikoassessments und deren Behandlung
- Perform

27001 Anh

- Contro
- Contro
- Contro
- Control 6.3 Information security awareness, education and training
- Control 8.13 Information Backup

ISO 27001 hilft bei NIS-2!

BSI 200-4

Anforderungskatalog zum BSI-Standard 200-4 gibt einen komprimierten Überblick zu allen MUSS- und SOLLTE-Anforderungen des Standard-BCMS.

DIN SPEC 27076

Organisation, Kenntnisse und Management für Notfälle sind Teil der Analyse

TISAX Anforderungen

- **Control: 1.2.1**

  Die Wirksamkeit des ISMS wird regelmäßig durch das Management überprüft.→ Ergebnisse Notfallübungen

- **Control 1.4.1**

  Es existiert eine Vorgehensweise, wie Informationssicherheitsrisiken innerhalb der Organisation identifiziert, beurteilt und behandelt werden.
- Kriterien für die Beurteilung und Behandlung von Informationssicherheitsrisiken sind vorhanden.
- Maßnahmen zur Behandlung von Informationssicherheitsrisiken und deren Verantwortliche sind festgelegt und dokumentiert. Es existiert ein Maßnahmenplan bzw. Statusübersicht der Maßnahmenumsetzung.
- Bei Änderung des Umfelds (z. B. Organisationsstruktur, Standort, Änderung von Regelwerken) erfolgt eine zeitnahe Neubewertung.

Weitere Anforderungen

DSGVO

- TOM´s, Meldepflicht 72h bei Datenschutzvorfall

NIS-2

- Prävention, Risikomanagement, Meldepflicht 24 h / 72 h / Laufend

Zahlungsdiensteaufsichtsgesetz (ZAG)

- Zahlungsdienstleister müssen die BaFin unverzüglich über schwerwiegende Betriebs- oder Sicherheitsvorfälle unterrichten1

Risikomanagementpflichten und Meldepflichten

- § 91 Abs. 2 AktG Einrichtung eines Risikofrüherkennungs- und Überwachungssystems für bestandsgefährdende Risiken
- § 91 Abs. 3 AktG Vorstand einer börsennotierten Gesellschaft ist verpflichtet, ein angemessenes und wirksames Internes Kontrollsystem und Risikomanagementsystem einzurichten.
- Sorgfaltspflichten des Vorstands einer AG (§ 93 AktG) sowie eines jeden GmbH-Geschäftsführers (§ 43 Abs. 1 GmbHG) zum Schutz der Gesellschaft sind einzuhalten, sonst bestehen Risiken der persönlichen Haftung
- Meldepflichten am Kapitalmarkt

Warum Notfallplan

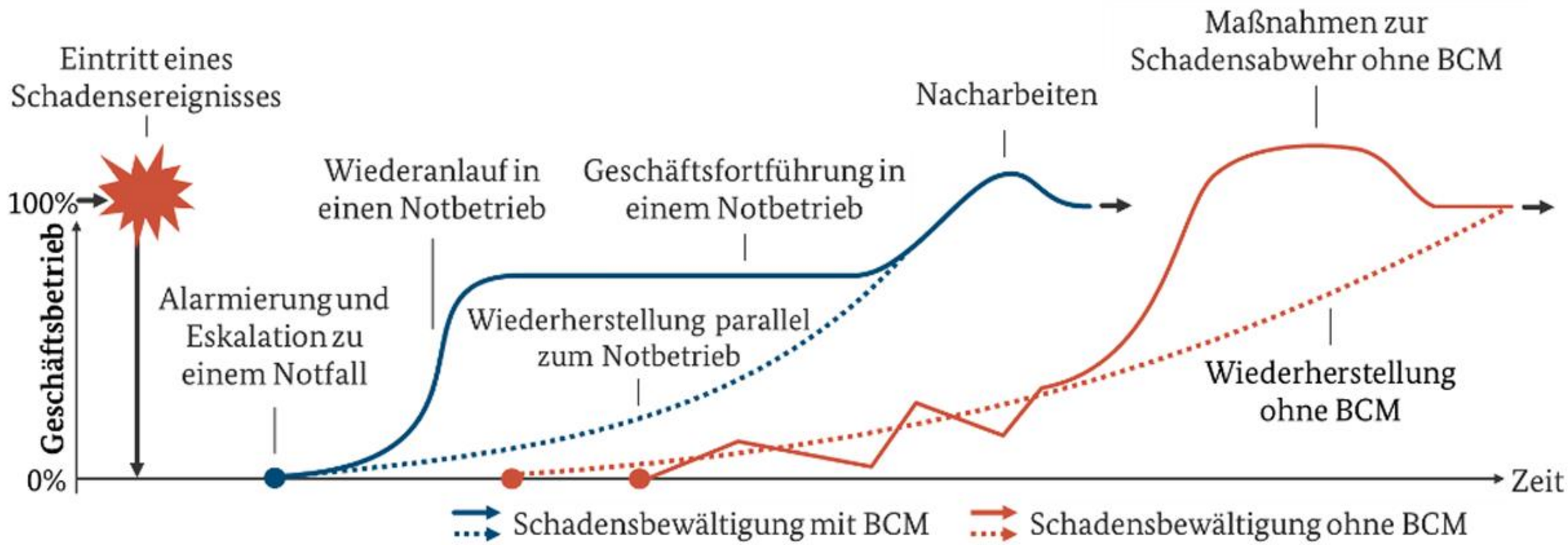


Abbildung 5: Bewältigung eines schwerwiegenden Schadensereignisses mit und ohne BCM

Quelle: BSI

Notfallmanagementrisiken

- Handeln unter Druck und mit hohem Risiko
- Verfügbarkeit der nötigen Informationen (aktuell, auch ausgedruckt?)
- Mangelnde Regelungen für Zuständigkeiten und Eskalationswege
- Ansprechpartner sind nicht erreichbar, Kommunikation und Vertretungen sind nicht geregelt
- Notfallplan nicht verfügbar, Entscheidungsprozesse unklar
- Remotezugänge nicht dokumentiert
- Logdateien fehlen oder sind zu jung (Fehlerfall und Gegenwart) oder wurden nie für den Fehlerfall geprüft bzw. laufend gesichtet

Cloud

- Cloud Lösungen müssen klar beschrieben sein
- Cloud Lösungen sind nicht automatisch sicherer
- Cloud-Anbieter machen nicht automatisch Backup oder langfristige Archivierung
- Backup ist in eigener Verantwortung
- Archivierungen müssen auf Basis eines Konzept erstellt werden (wie lange, was, wer, wie, Prüfungen etc.) und auf das Risiko abgestellt sein

Backup

- Backup-Methode (Vollsicherung, Teilsicherungen, 3-2-1= 3 Kopien, 2 unterschiedliche Medien, 1 örtlich getrennt ohne Netz)
- Sicherungsintervalle (Permanent, Täglich, Wöchentlich etc.)
- Speichermedien (Festplatten, Tapes, Cloud, neue Medien oder rollierend)
- Best Practices (Risikobewertung, Fristen, Recovery-Plan, Backup-Restore-Tests, Dokumentation, Rechtspflichten, Schulung der Mitarbeiter, übergeordnetes Sicherheitskonzept)
- Wirtschaftlichkeit (Kosten Betrieb und Wiederherstellung vs. Schaden)
- Versicherungsanforderungen
- **Achtung:** Cloud und Ransomware bedenken

Backup

- Backup-Methode (Vollsicherung, Teilsicherungen, 3-2-1= 3 Kopien, 2 unterschiedliche Medien, 1 örtlich getrennt ohne Netz)
- Sicherun
- Speiche lierend)
- Best Pra Restore-Tests, Dokume eordnetes Sicherhe
- Wirtschaftlichkeit (Kosten Betrieb und Wiederherstellung vs. Schaden)
- Versicherungsanforderungen
- **Achtung:** Cloud und Ransomware bedenken

Kein Backup – Kein Mitleid

Notfallüberlegungen

- **Klare und dokumentierte Zuständigkeiten**
- Nicht nur auf Qualität und Engagement der IT **hoffen**
- **Risikoorientierte** Szenarien vorgeplant
- Keine **einzelnen Abhängigkeiten** schaffen (z. B. auf einen Experten)
- Klare **Kommunikationsplanung** / Kommunikation „mit einer Stimme“
- Mindestens einmal/Jahr **Übung** und Aktualisierung (mit Brandschutzübung?)
- Externe Partner für Notfälle sind **im Vorfeld definiert und bekannt**, ggf. über Rahmenverträge gebunden (inkl. Plan B, falls Plan A nicht verfügbar)
- Externe Dienstleister haben **aktuelle Dokumente**, Liste der AP ist aktuell, vice versa hat dieser alles über Sie verfügbar
- **Forensik**: Planung und Regeln für Logs liegen vor (App-Logs, Powershell, Proxy/Firewalls) mit genug Zeitpuffer (mindestens 6 Monate rückwirkend)

Mindeststandards KMU

- 14 Fragen im Cyber-Sicherheits-Check für KMU (BSI)
  https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Cyber-Sicherheit_KMU.pdf?__blob=publicationFile&v=10
- Mittelstand Digital: Cybersicherheit – Prävention und Angriffsszenarien für KMU
  https://www.zentrum-ilmenau.digital/cybersicherheit-praevention-und-angriffsszenarien-fuer-kmu/
- DIN SPEC 27076

Cybersicherheitscheck

14 Fragen im Cyber-Sicherheits-Check für KMU (BSI)

Frage 1: Wer ist verantwortlich?

Frage 2: Wie gut kennen Sie Ihre IT-Systeme?

Frage 3: Führen Sie regelmässig eine Datensicherung durch?

Frage 4: Spielen Sie regelmässig Updates ein?

Frage 5: Haben Sie Makros deaktiviert?

Frage 6: Verwenden Sie Virenschutzprogramme?

Frage 7: Haben Sie eine Richtlinie für sichere Passwörter festgelegt?

Frage 8: Haben Sie eine Firewall eingerichtet?

Frage 9: Wie sichern Sie Ihre Mailaccounts ab?

Frage 10: Wie trennen Sie unterschiedliche IT-Bereiche?

Frage 11: Haben Sie IT-Risiken im Homeoffice und bei Geschäftsreisen im Griff?

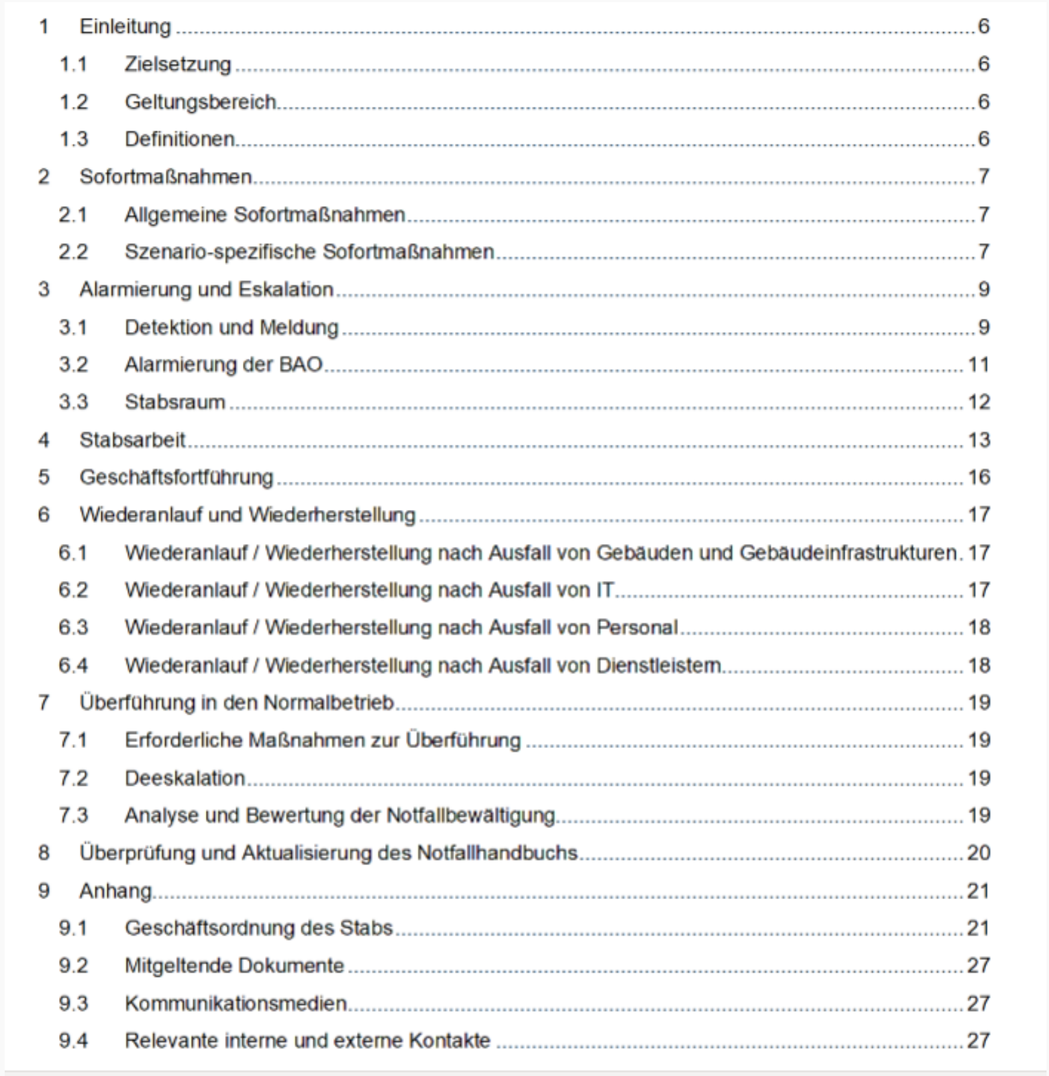
Frage 12: Wie informieren Sie sich und Ihre Beschäftigten?

Frage 13: Deckt Ihre Versicherungspolice auch Cyber-Risiken ab?

Frage 14: Wissen Sie, wie Sie bei einem Cyber-Angriff reagieren müssen?

Notfallhandbuch

- Umfang selbst entscheiden
- Vorlagen vorhanden (u.a. BSI 200-4)
- Mindeststandard
- Wichtigste Szenarien „vordenken“
- Auffindbarkeit des Handbuchs
- Aktualität des Notfallhandbuchs
- Dokumentationen in Papierform im Safe (Zugang, Aktualität)



Quelle: BSI

Rollen

- Geschäftsleitung
- Meldender des Notfalls
- Risikomanager
- Rechtsabteilung (externer Anwalt)
- ISB / CISO
- DSB
- Interne Verantwortliche (Fachbereiche, HR et.)
- Kommunikationsstellen
- Externe (Eigentümer, Dienstherren, Behörden, Polizei)

Übungen I

- Reale Simulation ist zu bevorzugen (Wirklichkeit!)
- Erkennen, was nicht gut (oder gar nicht) gelöst oder vergessen wurde
- Auswirkungen ohne Vorarbeiten unklar (Risiken? Was passiert wirklich?)
- Nur mit „Plan B“ für den Fehlerfall
- Nur mit stabilem Backup (Planung, Umsetzung, Vorhandensein, Restore geprüft, Wiederanlauf geprüft, Datenqualität geprüft, Zeitbedarf)
- Nur nach Abstimmung mit der Produktion
- OT sollte auch Übung machen
- Mehrfache Wiederholungen und wechselnde Szenarien wünschenswert

→ Angst vor Kosten, realen Verlusten und Produktionsausfall (nix anfassen)

Übungen II

Schreibtischübung

- 1 Fiktives Szenario (so real wie möglich)
- 2-4 h Dauer
- Alle Beteiligten am Tisch
- Mit Vorbereitung
- Teilsimulation
- Drehbuch mit Zeitangaben (Übung und real)
- Check Inhalte, Ablauf und Lücken
- Dokumentation und „Lessons learned“
- Mehrfache Wiederholungen möglich

→Übungen kosten Zeit und Geld, richtig! Aber was kostet Sie der Notfall ohne Übung?

Bearbeitung

- Aufnahme der Fakten
- Analyse Zuständigkeiten
- Analyse Fakten, Ursachen und Folgen
- Zuweisung der richtigen Adressaten
- Gegenmaßnahmen (BAO, Kurz- und langfristig)
- Dokumentation
- Kommunikation
- Lessons learned / KVP

→ 10 – 10 – Regel: 10 Minuten Ruhe, Sammlung, Prüfung der Reihenfolge der nächsten 10 Minuten

Fragen & Entscheidungen

- Grundsatzentscheidungen (operativ, taktisch, strategisch)
- IT-Entscheidungen
- Produktionsentscheidungen (Stopp, Änderungen)
- Organisationsentscheidungen (Budget und Kaufprozess bei Kauf von IT-Hardware per sofort möglich? Auf Rechnung? Kreditkarte?)
- Kommunikationsentscheidungen (Mitarbeiter, Öffentlichkeit, Eigentümer, Kunden, Lieferanten, Behörden)
- Juristische Entscheidungen inkl. Datenschutz

→ Wichtige Entscheidungen, daher: **Notfälle sind Chefsache in KMU!**

Opexa™
Advisory

Was nehmen Sie aus dem Vortrag mit?

Fazit

- Nichts zu tun ist keine Option
- Gut vorbereitet sein schont die Nerven, beruhigt das Management und Eigentümer
- Risikomanagement ist Bestandteil eines ISMS (TISAX, ISO/IEC 27001) sowie weiterer Themen und Standards (DORA, Lieferketten usw.)
- Versicherungen schätzen Eigeninitiative
- Kulturelle Weiterentwicklung
- Übung macht den Meister

Dank Notfallplan ruhig schlafen!

Opexa™
Advisory

Nun können Sie sich auf den Weg machen, “Ihr” Notfallmanagement aufzubauen

Opexa™
Advisory

Ende

Danke für ihre Zeit und Aufmerksamkeit

Opexa™
Advisory

Fragen?


Democratizing
Information
Security
www.opexaadvisory.de
Opexa™
Advisory
Please hold the handrail
Please stand on the right

Kontaktdaten

Opexa Advisory GmbH

Franz-Joseph-Straße 11

D-80801 München

+49 89 9018 0448

Office@opexa.de

www.opexaadvisory.de

Klaus Kilvinger

Geschäftsführer

Disclaimer

- Die in diesem Vortrag genannten Produkte und Marken dritter und die die Rechte an den Fotos gehören den Eigentümern der jeweiligen Markenrechte. Alle anderen Rechte an dem Vortrag liegen bei der Opexa Advisory GmbH. TISAX – Namensrechte liegen bei der ENX Association
- Alle Informationen in diesem Dokument wurden nach bestem Wissen und Gewissen zur Einführung in das Thema erstellt, die Aussagen/Empfehlungen erfolgen ohne Gewähr und sind teils interpretationsfähig, sie erheben keinen Anspruch auf inhaltliche Vollständigkeit und Richtigkeit. Die Inhalte stellen keine Rechtsberatung dar.
- Der Vortrag wurde von der Opexa Advisory GmbH erstellt und kann von den Teilnehmern des Webinars für interne Zwecke verwendet werden, jegliche Weitergabe, Kopie oder sonstige unautorisierte Verwendung ist untersagt und eine Verwendung nur nach Rücksprache mit dem Autor erlaubt.