Opexa™ Advisory

IT-Notfallplanung

Bereit sein, wenn die Krise eintritt!

IHK – Webinar

11.10.2023

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, BVMW (u.a.)
- Langjährige Expertise im Bereich IT-Serviceindustrie und Software-Qualitätssicherung mit umfangreicher Führungserfahrung

Opexa Leistungen

- Fokus zu 100 % auf **Informationssicherheitsmanagement für KMU**
- **Umfassende Begleitung** unserer Kunden bei der Implementierung eines ISMS (ISO 27001, TISAX®, B3S)
  - Erläuterung der Anforderungen und „Übersetzung“ des Inhaltes, GAP-Analysen
  - Vorbereitung auf Audits und Auditbegleitung und Support bei Beseitigung der Abweichungen
- Consulting zum **Business Continuity Management** (ISO 22301, BSI 200-4)
- Seminare zu **ISO 27001** und **TISAX®** (inhouse und online)
- Services zur **DIN SPEC 27076**
- **ISB/CISO as a Service** („Ciso a la carte®“)
- Beratung und Betrieb von **Hinweisgebersystemen**
- Support **Einführung ISMS Lösungen**
- Sonstige begleitende Services für Informationssicherheit (Pentest, Schwachstellenscans, Phishing Kampagnen, Awareness)

Fachpublikationen

Fortlaufend Artikel und Veröffentlichungen in Fachzeitschriften wie QZ Magazin, DGQ-Blog, Fachbüchern, Tagungsbänden, usw.

- 10/2023 QZ-Magazin
  Gute Software braucht klare Kriterien
  Wie ISO 25010 der Qualität in der Softwareentwicklung dient
- 08/2023 QZ-Magazin
  Ziel: Business Continuity Management
  Was zur Umsetzung der NIS-2-Richtlinie zu beachten ist
- 01/2023 QZ-Magazin
  Hase und Igel im Cyberspace
  Informationssicherheit bleibt immer ein „Infinite Game“
- 10/2022 QZ-Magazin
  Starke Kombi: QM und Informationssicherheit
  Warum QM und Informationssicherheitsmanagement zusammengehen

oder tagesaktuell siehe

- www.opexaadvisory.de/brainfood/categories/veröffentlichungen
- www.ThomasSalvador.com/Veröffentlichungen

DORA Tagung

In Kooperation mit Management Circle

- Versicherungen, Banken, Fondsgesellschaften, etc.
- DORA ist eine Ergänzung zu VAIT, BAIT, KAIT
- Keine gänzliche neue Regulierung, aber Konkretisierung und Erweiterungen (u.a. Cloud)
- Testaufwand und Prüfungen deutlich erweitert (u.a. szenariobasierte Tests, Kompatibilitätstests, Leistungstests,)
- Ganzheitlicher, vorausschauender Ansatz empfehlenswert
- Ab 1/2025 verpflichtend

Link: [Seminar: DORA - IT-Risiken im Fokus der Aufsicht | Management Circle]

Ausbildungsinitiative

Unsere Experten entwickeln Seminare und führen diese mit *namhaften und ausgewählten Partnern* durch.

Aktuelle Formate und Themen:

heise Academy

heise Academy: Online Weiterbildung für IT-Professionals

Ab Oktober 2023 **"TISAX– sichere Datenübertragung in der Automobilindustrie“**

DGQ Deutsche Gesellschaft für Qualität + VDA QMC Qualitäts Management Center im Verband der Automobilindustrie

DGQ Anlaufstelle Nr. 1 für Fortbildungen im Bereich Managementsysteme und Qualität

- ISO 27001:2022 Update
- **ISO 27001:2022 Implementer** (ab Q3/2023)
- TISAX® Training - Foundation Level
  (Seit 2018! First Mover. Weltweit erstes TISAX Training)
- Informationssicherheitsbeauftragter Automotive (ISB-A)

Metatrends / Regulatorik

Infosec Bedrohungen wachsen

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

Demographie

Weniger Arbeitskräfte, Wissen geht in Rente, Wissensmangel zum Organisationswissen, zu langsames Lernen

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

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

EU-Maschinenrichtlinie NEU

- KI-Risiken sind zu berücksichtigen
- Cybersicherheit

Notfall

- Umfeld
- Studien
- Definition
- Umsetzungsrahmen
- Reifegrad
- Normen und Standards, Gesetze
- Notfallmanagementrisiken
- Notfallhandbuch
- Übungen
- Fazit

BSI Empfehlungen

Cyber-Sicherheit ist Chefsache!

Informationssicherheit ist ein strategisches Thema und damit eine Leitungsaufgabe für das Topmanagement.

Cyber-Resilienz erhöhen!

Bereiten Sie Ihr Unternehmen auf mögliche Vorfälle vor. Halten Sie Übungen ab, spielen Sie regelmäßig neue Szenarien durch.

Managen Sie Cyber-Risiken!

Machen Sie kontinuierliche Bestandsaufnahmen der konkreten Bedrohungslage Ihres Unternehmens und setzen Sie entsprechende technische, organisatorische und prozessuale Schutzmaßnahmen um.

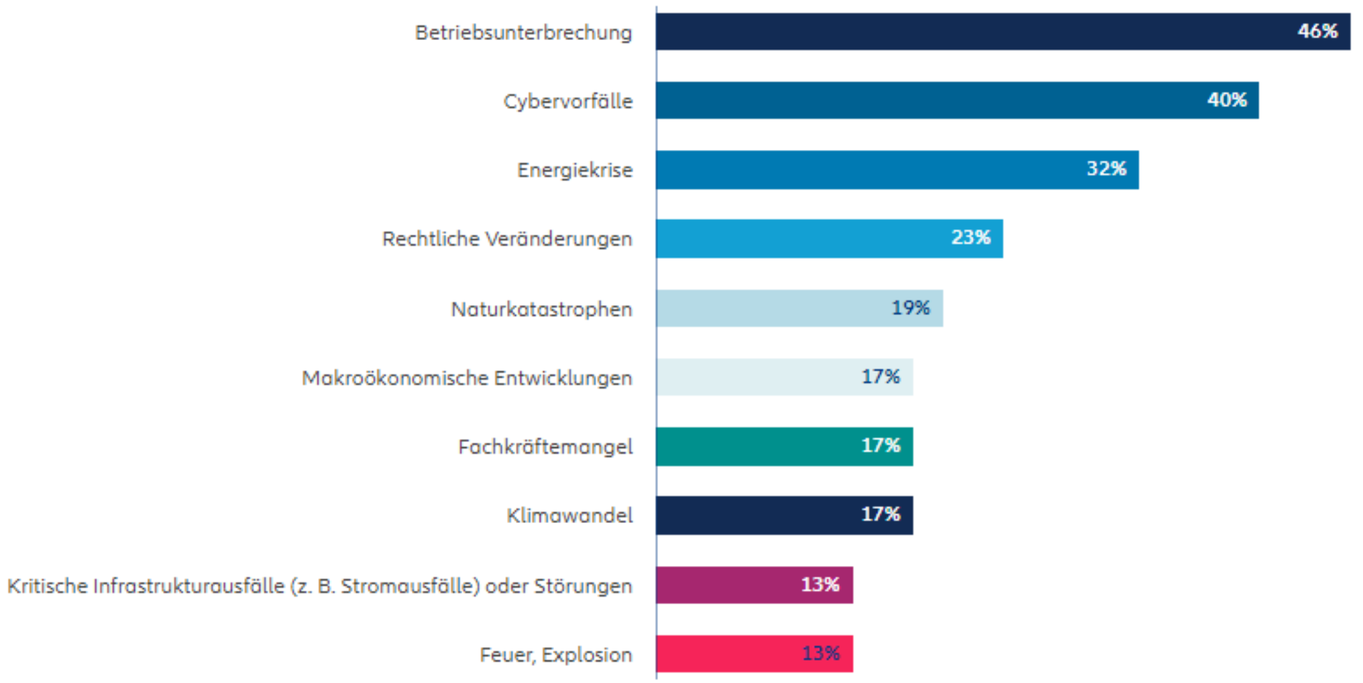
Situation - DE

Allianz

Top 10 Geschäftsrisiken in Deutschland in 2023

Allianz Risk Barometer 2023

Die Zahlen geben an, wie oft ein Risiko als Prozentsatz aller Antworten für das jeweilige Land ausgewählt wurde: 384. Die Zahlen addieren sich nicht zu 100%, da bis zu drei Risiken ausgewählt werden konnten.



AGCS News & Insights

Quelle: Allianz Global Corporate & Specialty

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)?

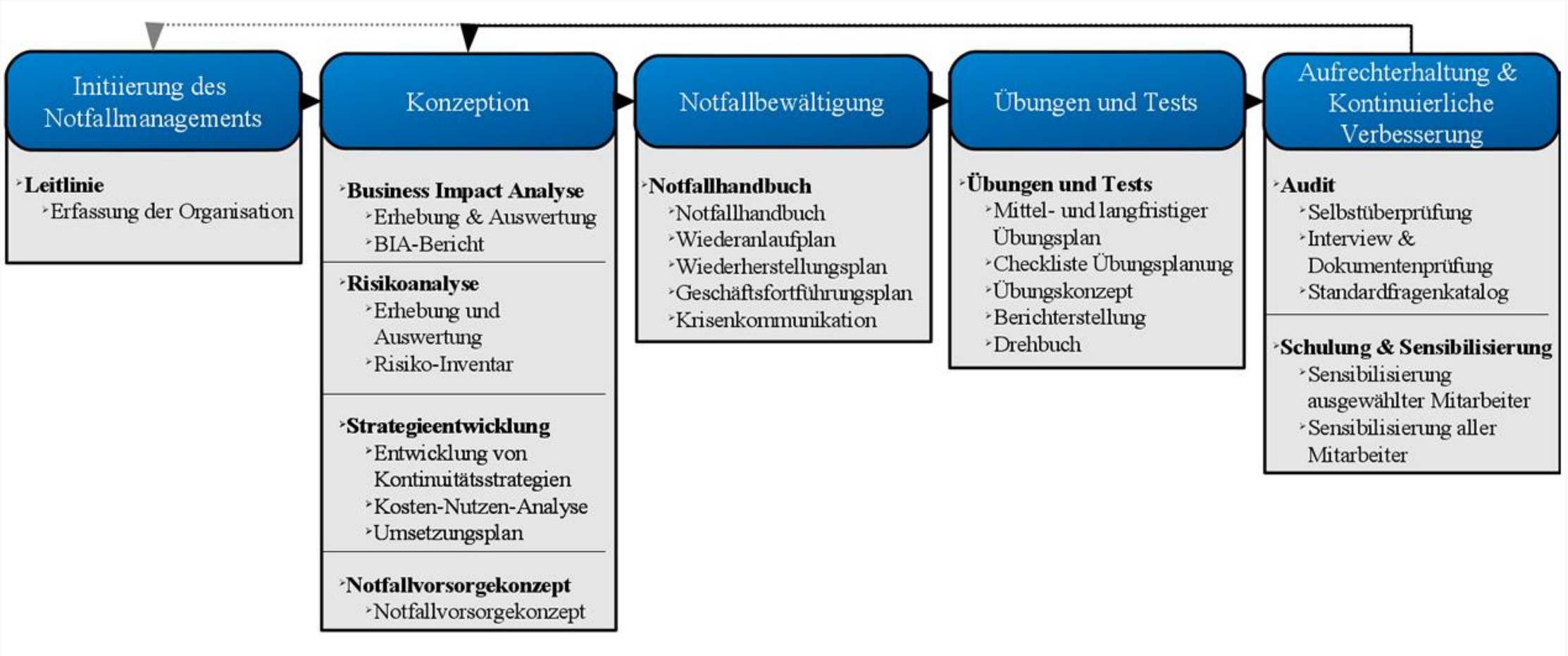
50% wichtig, 37% bedingt wichtig, Rest „nicht wichtig“ oder „keine Angabe“

Definitionen

Vorfallsart	Erläuterung	Behandlung
Einfache Störung	Kurzzeitiger Ausfall von Prozessen oder Ressourcen mit nur geringem Schaden	Behandlung ist Teil der üblichen Störungsbehebung
Notfall	Länger andauernder Ausfall von Prozessen oder Ressourcen mit hohem oder sehr hohem Schaden	Behandlung verlangt besondere Notfallorganisation
Krise	Im Wesentlichen auf die Institution begrenzter verschärfter Notfall, der die Existenz der Institution bedroht oder die Gesundheit oder das Leben von Personen beeinträchtigt	Da Krisen nicht breitflächig die Umgebung oder das öffentliche Leben beeinträchtigen, können sie, zumindest größtenteils, innerhalb der Institution selbst behoben werden
Katastrophe	Räumlich und zeitlich nicht begrenztes Großschadensereignis, zum Beispiel als Folge von Überschwemmungen oder Erdbeben	Aus Sicht einer Institution stellt sich eine Katastrophe als Krise dar und wird intern durch deren Notfallorganisation in Zusammenarbeit mit den externen Hilfsorganisationen bewältigt

Quelle: BSI

BSI 100-4 Umsetzungsrahmen



Quelle: BSI

BSI 100-4 Reifegrad

Umsetzungsgrad III:

- Vollständige Bearbeitung aller Phasen des Notfallmanagements

Umsetzungsgrad II:

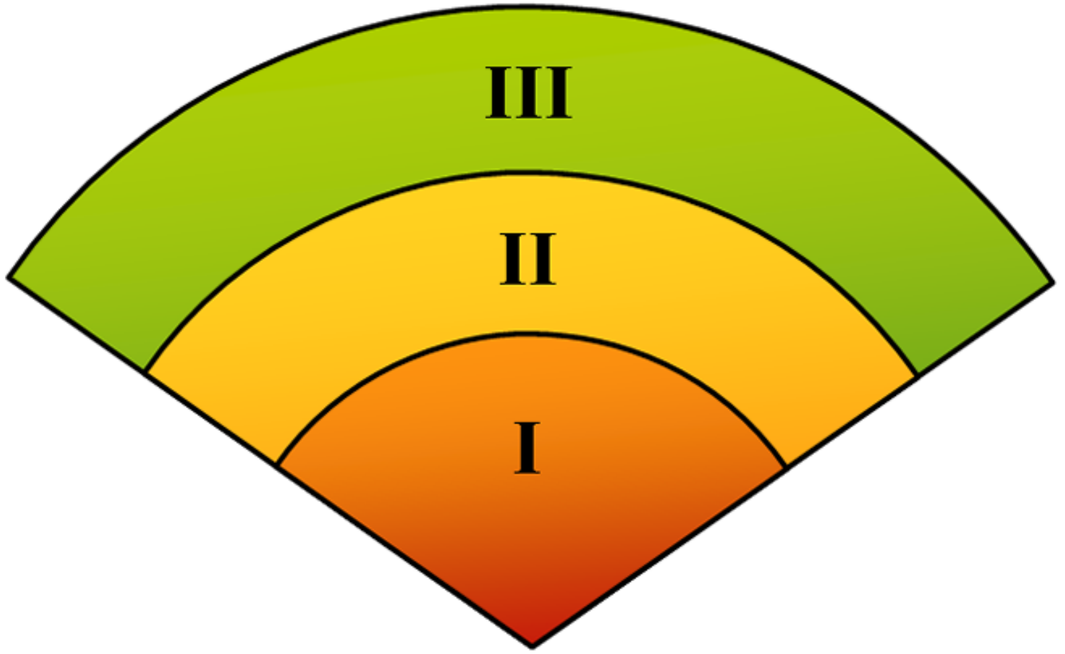
- Präventive und reaktive Notfall-reaktion definiert und beschrieben
- Übungen und Tests sowie kontinuierliche Weiterentwicklung in Grundsätzen beschrieben

Umsetzungsgrad I:

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

Entwicklungszeitraum

Ressourceneinsatz



Quelle: BSI

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

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 schreibt die Einführung eines Risikomanagementsystems vor
- Sorgfaltspflichten des Vorstands einer AG (§ 93 AktG) sowie eines jeden GmbH-Geschäftsführers (§ 43 Abs. 1 GmbHG)

Notfallmanagementrisiken

- Handeln unter Druck und mit hohem Risiko
- Verfügbarkeit der nötigen Informationen
- Mangelnde Regelungen für Zuständigkeiten und Eskalationswege
- Ansprechpartner sind nicht erreichbar, 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
- Backup nicht verfügbar oder korrupt (Empfehlung 3-2-1-Modell: Mindestens drei Datenkopien, Speicherung der Daten auf mindestens zwei verschiedenen Medien, eine Backup-Kopie an einem externen Standort)

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

→ Häufigste Probleme sind Desinteresse, Faulheit, Angst vor der Meldung (Denunziantentum, Folgeaufwand, Ärger, Zeitverlust, Vorwürfe) oder Unkenntnis der Meldewege

→ Awareness ist wichtig

Notfall – bitte nicht

- Hektik und Aktionismus
- „Alle Stecker ziehen“
- Eigene Reparaturversuche
- Verfrühte, unüberlegte Statements nach innen & außen

Notfall – bitte ja

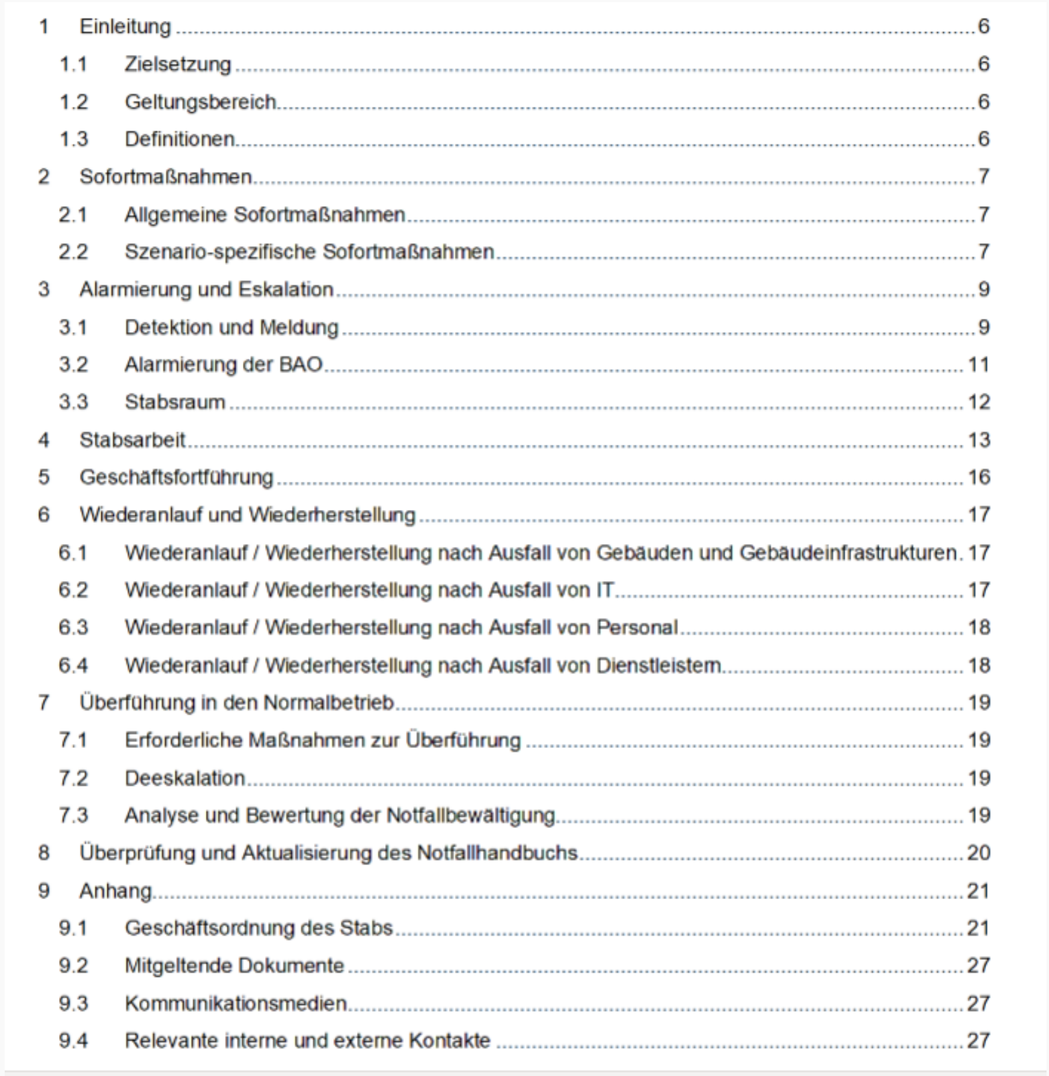
- Ruhe bewahren
- Klare, eindeutige Anweisungen an Belegschaft
- Schnelle und ehrliche Kommunikation mit Kunden und Partnern
- Gesetzlich kritische Themen mit Anwälten abstimmen

Notfallüberlegungen

- Klare und dokumentierte Zuständigkeiten
- Nicht nur auf IT hoffen
- Risikoorientierte Szenarien vorgeplant
- Keine einzelnen Abhängigkeiten schaffen (z. B. auf einen Experten)
- Klare Kommunikationsplanung / Kommunikation „mit einer Stimme“
- Mindestens einmal pro Jahr Übung mit Probealarm und Aktualisierung
- 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 und Liste der AP ist aktuell, vice versa hat dieser alles über Sie
- Planung und Regeln für Logs liegen vor (App-Logs, Powershell, Proxy/Firewalls) mit genug Zeitpuffer (mindestens 6, besser 12 Monate)

Notfallhandbuch

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



Quelle: BSI

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 (Geplant, Umgesetzt, 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 realen Verlusten und Produktionsausfall

Übungen II

- Fiktive Szenarien mit hohem Wirklichkeitsbezug (1-3 in initialer Phase)
- Alle Beteiligten am Tisch (außer bei Teilübungen)
- Teilsimulationen möglich
- Check Inhalte, Ablauf und Lücken
- Dokumentation und „Lessons learned“
- Simulation ersetzt keine „reale“ Übung
- Mehrfache Wiederholungen und wechselnde Szenarien

Übungen III

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?

Fazit

- Risiken ernst nehmen (Die Frage ist nicht, ob, sondern wann sie getroffen werden)
- Szenarien definieren (so real wie möglich, Anzahl und Detail sind skalierbar)
- Alle Beteiligten am Tisch, der „Plan B“ kann somit für alle transparent werden
- Thema im Rahmen des Risikomanagements für viele Anforderungen wichtig (DIN SPEC 27076, NIS2, ISO/IEC 27001, TISAX, ISO 22301 usw.), u.a. auch für Cyberversicherungen (Prämienberechnung)
- Gesamt-Information des Unternehmens (ISMS, weitere Dokumente) wichtig
- Notfall-Konzepte müssen dokumentiert und aktuell sein
- Menschliche Schwächen kompensieren (Prof. Ebbinghaus: Nach 6 Tagen kommt die Vergessenskurve auf 23 %. Konstant bleiben nur 15 % des Wissens erhalten)
- Kosten und Aufwand skalierbar (Wenige Grundlagen und Basisarbeit sind Minimum)
- Lerneffekt über den internen Reifegrad darf nicht unterschätzt werden
- Übung macht den Meister

Opexa™ Advisory

--ENDE—

Danke für Ihre Zeit und Aufmerksamkeit

Disclaimer

- Die in diesem Vortrag genannten Produkte und Marken dritter gehören den Eigentümern der jeweiligen Markenrechte. Alle anderen Rechte an dem Vortrag liegen bei der Opexa Advisory GmbH.
- Die Rechte an TISAX® gehören der ENX Association.
- Die Informationen wurde nach bestem Wissen und Gewissen zusammengestellt und deren Anwendung erfolgt ohne Gewähr.
- Die in diesem Vortrag vermittelten Informationen stellen keine Rechtsberatung dar.