K&K NETWORKS

IT-Notfallmanagement und Cybersicherheit für KMU und Kommunen: Strategien zum Schutz und zur Krisenbewältigung

Unna, April 2025

Ihr kompetenter IT-Partner

K&K NETWORKS GMBH

IST EIN HERSTELLERUNABHÄNGIGES
IT-SYSTEMHAUS & -LÖSUNGSANBIETER

K&K NETWORKS GMBH

WURDE 1993 GEGRÜNDET UND IST ÜBER
30 JAHRE ERFOLGREICH AM MARKT

KOMPETENZEN

- IT MANAGED SERVICES
- IT & CYBER SECURITY SERVICES
- IT INFRASTRUKTUR
- CABLING SOLUTIONS
- DATENSCHUTZ

Wieso überhaupt?

Datum	Betroffene	Land	Sicherheitsvorfall
04.04.2025	Rheinmetall	DE	Ransomware-Gruppe stiehlt angeblich 750 GB, veröffentlicht Datenprobe. » Details
02.04.2025	Spectos GmbH	DE	Daten-Analyst bestätigt mehrtätige Angriffe. » Details
01.04.2025	Anstalt für Kommunale Datenverarbeitung in Bayern (AKDB)	DE	Störung im Rechenzentrum: Kfz-Zulassungen zeitweise nicht möglich. » Details
01.04.2025	Fotostudio	DE	Ransomware-Gruppe erpresst angebliches Opfer um unbekannte Summe. » Details
01.04.2025	Heilbronn Marketing GmbH (HMG)	DE	Ransomware-Angriff: Kundendaten möglicherweise betroffen. » Details
	Büro-Systemlösungsbetrieb	DE	Ransomware-Gruppe macht Angriffsbehauptungen, droht mit Datenleak. » Details
	Tierarztpraxis	DE	Ransomware-Gruppe will 7,3 GB erbeutet haben. » Details
	Fachgroßhandel für Hygiene- und Reinigungssysteme	DE	Fachgroßhändler für Sauberkeit und Hygiene auf Opferblog gelistet. » Details
	Schuhhändler	DE	Schuheinzelhändler auf Opferliste von Ransomware-Gang aufgetaucht. » Details
	Maklerunternehmen	DE	Makler angeblich mit Ransomware attackiert

The most important business risks in 2025: global

Ranking changes are determined by positions year-on-year, ahead of percentages.

Rank		Percent	2024 rank
1	Cyber incidents *(e.g., cyber crime, IT network and service disruptions, malware / ransomware, data breaches, fines, and penalties)*	38%	*1 (36%)*
2	Business interruption *(incl. supply chain disruption)*	31%	*2 (31%)*
3	Natural catastrophes *(e.g., storm, flood, earthquake, wildfire, extreme weather events)*	29%	*3 (26%)*
4	Changes in legislation and regulation *(e.g., new directives, protectionism, environmental, social, and governance, and sustainability requirements)*	25%	*4 (19%)*
5	Climate change *(e.g., physical, operational, and financial risks as a result of global warming)*	19%	*7 (18%)*
6	Fire, explosion	17%	*6 (19%)*
7	Macroeconomic developments *(e.g., inflation, deflation, monetary policies, austerity programs)*	15%	*5 (19%)*
8	Market developments *(e.g., intensified competition / new entrants, M&A, market stagnation, market fluctuation)*[1]	14%	*9 (13%)*
9	Political risks and violence *(e.g., political instability, war, terrorism, coup d'état, civil unrest, strikes, riots, looting)*	14%	*8 (14%)*
10	New technologies *(e.g., risk impact of artificial intelligence, connected / autonomous machines)*	10%	*12 (9%)*
11	Shortage of skilled workforce[2]	9%	*10 (12%)*
12	Critical infrastructure blackouts *(e.g., power disruption)* or failures *(e.g., aging dams, bridges, rail tracks)*	9%	*13 (8%)*
13	Energy crisis *(e.g., supply shortage / outage, price fluctuations)*	8%	*11 (12%)*
14	Theft, fraud, corruption[3]	7%	*14 (7%)*
15	Loss of reputation or brand value *(e.g., public criticism)*	7%	*15 (6%)*
16	Insolvency[4]	6%	*17 (5%)*
17	Environmental risks *(e.g., pollution, biodiversity issues, resource scarcity)*	6%	*16 (5%)*
18	Product recall, quality management, serial defects	4%	*17 (5%)*
19	Pandemic outbreak *(e.g., health and workforce issues, restrictions on movement, cancellation of events)*	3%	*19 (4%)*
	Other	*3%*	

Foto: Allianz Commercial

https://www.security-incidents.de/sicherheitsvorfall-daten

bitkom

Presseinformation August 2024

Angriffe auf die deutsche Wirtschaft nehmen zu

- **8 von 10 Unternehmen von Datendiebstahl, Spionage oder Sabotage betroffen**
- **Rekordschaden von rund 267 Milliarden Euro**
- **China wird immer mehr zum Standort Nr. 1 für Angreifer**
- **Cyberangriffe: Zwei Drittel der Unternehmen fühlen sich in ihrer Existenz bedroht**

Gesetzliche Anforderungen:

- DSGVO (Datenschutz-Grundverordnung)
- NIS2-Richtlinie (Netz- und Informationssicherheit)
- eIDAS-Verordnung (elektronische Identifizierung und Vertrauensdienste, z. B. digitale Signaturen, Zeitstempel)
- EU Cybersecurity Act (Rahmen für EU-weite Zertifizierungen in der IT-Sicherheit
- Digital Operational Resilience Act (DORA, insbesondere für Finanzsektor)
- KI-Verordnung
- … sowie eine Vielzahl von branchenspezifischen Richtlinien und Zertifizierungsanforderungen

Maßnahmen

IT-Sicherheit für KMUs & Kommunen

- Netzwerksicherheit
- Zugangs- und Benutzerverwaltung
- Notfallmanagement
- Backup
- Endgeräte- & Softwareschutz
- Datenschutz
- Sicherheits-überprüfungen
- IT-Sicherheits-schulungen
- E-Mail-Sicherheit
- Monitoring

K&K NETWORKS

CyberRisikoCheck

nach DIN SPEC 27076

Was ist der CyberRisikoCheck?

Das **Bundesamt für Sicherheit in der Informationstechnik (BSI)** sichert Deutschlands IT-Infrastruktur, schützt staatliche und kritische Systeme und entwickelt Sicherheitsstandards. Es berät Behörden und Unternehmen und reagiert auf Cybervorfälle, um die Anwendung digitaler Technologien nachhaltig zu stärken.

Der **CyberRisikoCheck nach DIN SPEC 27076** ist ein neuer **Beratungsstandard des BSI** zur kosten- und zeiteffizienten Verbesserung der IT-Sicherheit in kleinen Unternehmen.

- Durchführung ausschließlich durch von **BSI-zugelassenen** IT-Dienstleistern
- Branchenunabhängige und bedarfsgerechte Beratung
- Konzipiert für Betriebe **bis 50 Mitarbeiter mit PC-Nutzung**
- Definiert 27 Anforderungen, um die relevantesten Risiken zu minimieren
- Erhebung in kurzen Sitzungen
- Ergebnisauswertung mit **Handlungsempfehlungen** zur Verbesserung der IT-Sicherheit

Vorteile des CyberRisikoCheck

Kleine Betriebe erhalten in sehr kurzer Zeit einen Überblick über ihre **individuelle IST-Situation zur Cybersicherheit**.

Nach Abschluss des CyberRisikoChecks haben die Unternehmen:

- Ihren **individuellen Risiko-Statuswert** (Score-Wert) inkl. Visualisierung der Schwachpunkte
- Eine Übersicht der umzusetzenden **Handlungsempfehlungen** und deren Priorisierung
- Hinweise auf **relevante Förderprogramme**, die finanziell bei der Umsetzung unterstützen

Unternehmen können ihren Qualitätsstandard ggü. Dritten (Auftraggebern, Investoren, Banken, Versicherungen, ...) nachweisen.

Die sechs Themenbereiche des CyberRisikoCheck

Organisation & Sensibilisierung

Betrachtet das managementseitige Engagement, sowie die Kompetenz-verteilung und Sensibilisierung von Mitarbeitenden

Identitäts- und Berechtigungsmanagement

Regelt die Zugangs- und Zutritts-berechtigungen (virtuell, physisch)

Datensicherung

Beschreibt Zuständigkeit, Umfang, Häufigkeit und Verfügbarkeit von Daten und deren Backups

Patch- und Änderungsmanagement

Prüft die Verfügbarkeit von Aktualität von eingesetzter Hard-/Software

Schutz vor Schadprogrammen

Behandelt die Haupteinfallstore für Schadsoftware

IT-Systeme und Netzwerke

Definiert die Sicherheitsmechanismen hinter der eingesetzten Informations- und Kommunikationstechnik

Ablauf des CyberRisikoCheck

Die IT-Sicherheitsberatung erfolgt in vier Schritten, welche Online, in Präsenz oder Hybrid durchgeführt werden können:

- **Gespräch zur Erstinformation** (1 Std.): Teilnehmer werden bestimmt, zeitlicher Rahmen fixiert, erste Unternehmensdaten aufgenommen, vorzubereitende Dokumente
- **Aufnahme des Ist-Zustandes** (2 – 3 Std.): Durchführung des ´semistrukturierten´ Interviews anhand des CyberRisikoCheck-Leitfadens mit 27 Anforderungen
- **Auswertung und Erstellung des Ergebnisberichts** (2 – 3 Std.): Ergänzung der Kommentare über den Interviewer und Durchführung der Bewertung
- **Präsentation der Ergebnisse** (1 – 2 Std.): Vorstellung des Ergebnisberichts, Erläuterung der Einzelergebnisse und der zu empfehlenden Maßnahmen, mögliche Nutzung von Fördermitteln

Ihr Kontakt zur Cyber-Sicherheit

Julius Appel
Geschäftsführer

K&K Networks GmbH

E-Mail: julius.appel@kuk-networks.de
Telefon: +49 2303 25400-12
Mobil: +49 177 2001319

LinkedIn: www.linkedin.com/in/julius-appel-074647183

IT-Notfallhandbuch

IT-Notfallhandbuch: „Was tun, wenn‘s brennt“?

- ***Nutzen und Zweck***
- ***Wichtige Bestandteile***
- ***Erstellung des Handbuchs***

Guido Wirtz,
Datenschutzbeauftragter (TÜV®)


ENCRYPTED
:56
stag, 16. Mai
HEWLETT-PACKARD

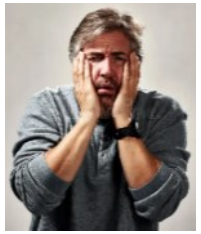
Ein (IT-) Notfall kann verschiedene Gründe haben

- Cyberangriffe von außen (Hacker)
- Angriffe von innen (Sabotage)
- Fahrlässige Systemnutzung / Fehlbedienung
- Technische Defekte, z.B. Ausfall der Klima-anlage im Serverraum, der Stromversorgung oder der Internet-Anbindung
- Blitzeinschlag/ Brand/ Wasserschaden
- Ausfall externer Cloud-Systeme

Und wie reagieren Sie ?

- **Wenn‘s brennt:**
  Die Feuerwehr anrufen

- **Bei Geistern:**
  die Ghostbusters rufen



- **Und bei**
  IT-Notfällen … ?

[Quelle: Pixabay]

Und wie reagieren Sie ?

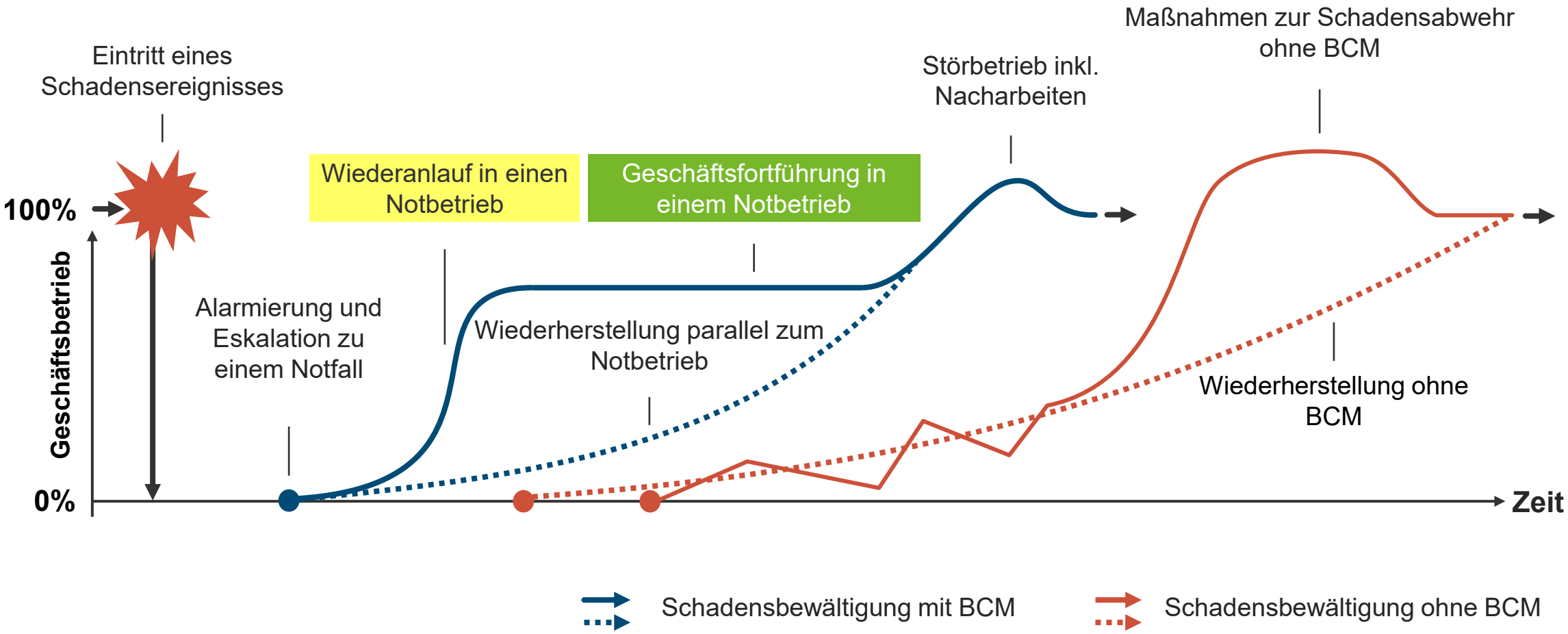
- **Wenn‘s brennt:**
  Die Feuerwehr anrufen
- **Bei Geistern:**
  die Ghostbusters rufen

- **Und bei IT-Notfällen:**
  IT-Notfallhandbuch!

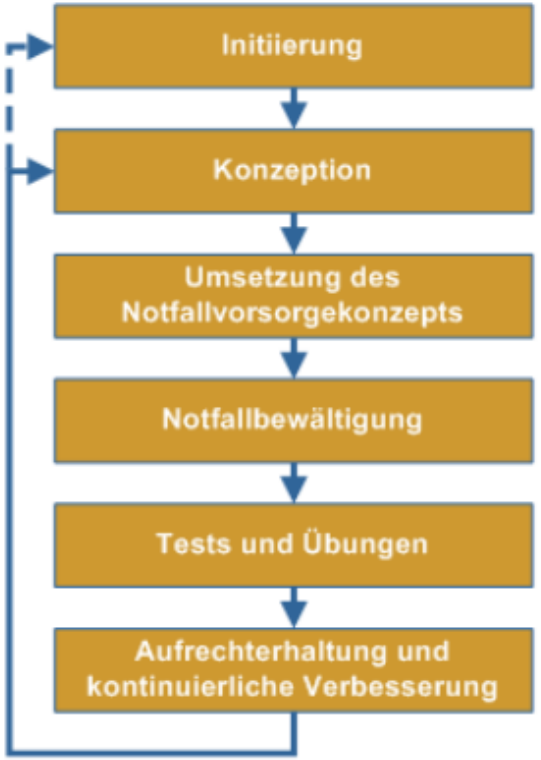
[Quelle: Pixabay]

Wer von Ihnen verfügt bereits über ein (IT-) Notfallhandbuch ?

Der Nutzen eines Notfallkonzepts („BCM“)

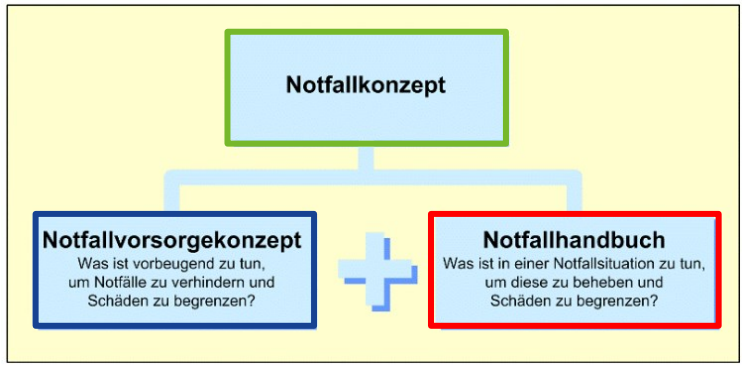


Die „Bibel“ zum Notfallmanagement (auch: *BCM* genannt): Der BSI-Standard 100-4



Das Notfallhandbuch ist Bestandteil des Notfallkonzepts

- **Ein Notfallkonzept besteht aus:**
  - **Notfallvorsorgekonzept:** präventiver Schutz gegen Notfälle und deren Auswirkungen
  - **Notfallhandbuch:** Handlungsanleitungen für Notfälle und Krisen



- **Wichtig: Drei Maßnahmen sind im Vorfeld des Notfallkonzepts erforderlich**
  1. **Business Impact Analyse:** Ermittlung der kritischen und hoch kritischen Geschäftsprozesse und Ressourcen sowie Kenngrößen für deren Wiederanlauf nach einer Panne
  2. **Risikoanalyse:** Untersuchung der Risiken für die kritischen Prozesse und Ressourcen
  3. Ableitung der jeweiligen **Kontinuitätsstrategie** zur Festlegung von **Notfall- und Notfallvorsorgemaßnahmen**

Hauptbestandteile eines IT-Notfallhandbuchs

- **Mitglieder des Krisenstabs**/ Ort und Ausstattung des **Lagezentrums**
- **Kontaktlisten:** Wichtige Ansprechpartner intern und extern (GF, IT-Support, IT-Dienstleister, IT-Hersteller, Cyberversicherung, Datenschutzbeauftragter etc.)
- **Kommunikationsleitfaden:** Wer informiert wen in welcher Reihenfolge, welche externen Stellen **MÜSSEN ggf. informiert** werden (NIS-2, Datenschutz)?
- **Anweisungen für den Notfall:** Sofortmaßnahmen und Anleitungen für typische Szenarien (z.B. Cyberangriff, Ausfall Internet, Ausfall ERP- oder E-Mail-System)
- **Inventarlisten** Ihrer Hard- und Softwaresysteme (inklusive Lizenzschlüsseln)
- **Zugangsdaten:** Hinweis, wo die Zugangsdaten für Ihre IT-Systeme abgelegt sind
- **Wiederanlaufpläne:** Prozesse zur teilweisen oder vollständigen systematischen Wiederherstellung der Geschäftsprozesse sowie dem Wiederanlaufen der IT-Systeme

Erstellung eines (IT-) Notfallhandbuchs

1. **Festlegung von Verantwortlichkeiten und Beteiligten durch die GF**
2. **Vorgelagert: Durchführung von Business Impact Analyse und Risikoanalyse, um potenzielle (IT-) Notfälle zu identifizieren**
3. **Benennung des Notfallbeauftragten, Festlegung der Mietglieder des Krisenstabes, Erstellung von Kontakt- und Inventarlisten**
4. **Erarbeitung der Notfallpläne für die einzelnen Szenarien, ggf. Optimierung von Sicherheitsmaßnahmen (Redundanzen etc.), bei Bedarf Festlegung von Kommunikationsmaßnahmen**
5. **Simulation bzw. Test der einzelnen Notfallpläne**
6. **Ableitung und Durchführung von Schulungen für die Mitarbeitenden**
7. **Regelmäßige Prüfung und Aktualisierung des Handbuchs**

Fazit: Nutzen eines (IT-) Notfallhandbuchs

- **Prophylaxe: Rechtzeitiges Erkennen möglicher Risiken und Definition von Gegenmaßnahmen**
- **Im Krisenfall: Minimierung von Ausfallzeiten der Produktion und weiterer Kernsysteme**

→ **Minimierung der resultierenden wirtschaftlichen Schäden für Ihr Unternehmen**

- **Projektnutzen:**
  „Der Weg ist das Ziel“

- **Noch Fragen? Dann gerne fragen.**
- **Ich freue mich auf die weiteren Gespräche mit Ihnen**

Dipl.-Ing. (TU) Guido Wirtz
Datenschutzbeauftragter (TÜV®)

K&K Networks GmbH
Otto-Hahn-Str. 44
59423 Unna

E-Mail: guido.wirtz@kuk-networks.de
Tel.: (02303) 25400-35


Q&A

K&K NETWORKS

Flexibel und bereit für die Zukunft