

ZUM AUSFÜLLEN UND AUSDRUCKEN

IT-Notfallhandbuch

Die zehn Abschnitte, die im Ernstfall gebraucht werden.
Ein Gerüst für Unternehmen, die noch keines haben.

UNTERNEHMEN

VERSION

STANDORT, FÜR DEN DIESES HANDBUCH GILT

STAND VOM

ERSTELLT VON

NÄCHSTE PRÜFUNG AM

VERANTWORTLICH FÜR DIE PFLEGE

FREIGEgeben VON (GESCHÄFTSFÜHRUNG)

Dieses Exemplar liegt an folgendem Ort:

AUSFERTIGUNG NR.

VON INSGESAMT

AUFBEWAHRUNGsort

Mindestens eine Ausfertigung gehört an einen Ort außerhalb der eigenen IT. Ein Notfallhandbuch, das als Datei auf dem Server liegt, ist bei einem Verschlüsselungsvorfall genau dann nicht erreichbar, wenn es gebraucht wird.

BEVOR SIE ANFANGEN

Wie Sie diese Vorlage benutzen.

Nehmen Sie sich einen halben Tag, nicht eine Woche. Ein unvollständiges Handbuch, das existiert, ist jedem vollständigen überlegen, das nie fertig wird.

In dieser Reihenfolge

- Zuerst Abschnitt 1 und die Notfallkarte. Damit ist der häufigste Fall abgedeckt: jemand merkt etwas und weiß nicht, wen er anrufen soll.
- Dann Abschnitt 9, die externen Ansprechpartner. Die Angaben haben Sie bereits, sie liegen nur verteilt.
- Dann Abschnitt 3, die kritischen Prozesse. Dieser Teil ist der anstrengendste und braucht die Geschäftsführung, nicht die IT.
- Der Rest folgt daraus.

Drei Regeln

- **Mobilnummern, keine Durchwahlen.** Bei Stromausfall ist die Telefonanlage tot.
- **Namen, keine Funktionsbezeichnungen.** „Der Systemadministrator“ hilft um drei Uhr nachts niemandem.
- **Gemessene Zeiten, keine geschätzten.** Alles, was Sie nicht getestet haben, ist eine Vermutung.

VORBEREITUNG

Notfallkarte zum Aushängen	3
----------------------------	---

DIE ZEHN ABSCHNITTE

1. Alarmierung: wer informiert wen, und wer entscheidet	4
2. Die ersten 30 Minuten: vier Szenarien	5
3. Kritische Prozesse und ihre Fristen	7
4. Abhängigkeiten	8
5. Wiederanlauf-Reihenfolge	9
6. Backup und Rücksicherung	10
7. Ausweicharbeitsplätze	11
8. Kommunikation nach außen und Meldefristen	12
9. Externe Ansprechpartner	13
10. Nachbereitung und Vorfallprotokoll	14

NACHWEISE

Übungsnachweis und Prüfprotokoll	15
Was dieser Vorlage noch fehlt	16

Was diese Vorlage nicht ist. Sie ist kein Notfallvorsorgekonzept und kein vollständiges BCMS nach BSI-Standard 200-4. Sie deckt die Notfallbewältigung ab, also das, was im Ereignisfall gebraucht wird, nicht die Vorsorgestrategie dahinter. Wenn Sie ein prüffähiges Managementsystem brauchen, ist das hier der Anfang davon, nicht das Ergebnis.

Die Gliederung folgt BSI-Standard 200-4, Kapitel 6.4, 6.9 und 6.10, und ist auf den Umfang eines Betriebs mit etwa 10 bis 150 Arbeitsplätzen gekürzt. Das Bundesamt für Sicherheit in der Informationstechnik stellt die amtliche Langfassung kostenlos bereit.

ZUM HERAUSTRENNEN

Notfallkarte.

Diese Seite kommt an die Wand, nicht in den Ordner. Neben den Drucker, in die Teeküche, in den Serverraum. Sie ist der einzige Teil des Handbuchs, den Menschen lesen, die nichts mit IT zu tun haben.



IM IT-NOTFALL

Erst melden. Dann nichts tun.

Keine Dateien löschen, keine Rechner neu starten, keine Passwörter ändern, bevor jemand von der Liste unten entschieden hat. Gut gemeinte Sofortmaßnahmen zerstören Spuren und verschlimmern den Schaden regelmäßig.

1. ANRUFEN: NAME

2. FALLS NICHT ERREICHBAR: NAME

MOBIL

MOBIL

UNSER IT-DIENSTLEISTER

NOTFALLNUMMER, RUND UM DIE UHR

Was Sie sagen sollten

Ihr Name und von welchem Gerät Sie anrufen. Was Sie beobachtet haben, wörtlich, ohne Deutung. Wann es angefangen hat. Wer es sonst noch bemerkt hat. Ob Sie vorher etwas angeklickt, installiert oder angesteckt haben. Letzteres ist keine Schuldfrage, sondern die wichtigste Angabe für die Eingrenzung.



Ein Satz, der sich lohnt. Ergänzen Sie mündlich, dass niemandem ein Vorwurf gemacht wird, der einen Vorfall meldet. Die durchschnittliche Verzögerung zwischen Bemerken und Melden entscheidet bei Verschlüsselungsvorfällen über den Umfang des Schadens, und sie ist fast immer eine Frage der Angst, nicht der Technik.

ABSCHNITT 1 VON 10

Alarmierung.

Wer wird in welcher Reihenfolge informiert, über welchen Weg, und wer entscheidet, dass ein Notfall vorliegt.

Meldekette

Von oben nach unten abarbeiten, bis jemand abnimmt. Mobilnummern eintragen, keine Durchwahlen.

ROLLE	NAME	MOBIL	ERREICHBAR	VERTRETUNG
1				
2				
3				
4				
5				

Wer erklärt den Notfall

Eine Störung wird vom Dienst behoben. Ein Notfall verändert Zuständigkeiten und Befugnisse. Jemand muss das aussprechen, sonst arbeiten alle weiter im Normalbetrieb.

ENTSCHEIDET ÜBER DIE NOTFALL-ERKLÄRUNG

VERTRETUNG, FALLS NICHT ERREICHBAR INNERHALB VON ___ MINUTEN

DARF EXTERNE HILFE BEAUFTRAGEN BIS ZU EINEM BETRAG VON

DARF ANORDNEN, SYSTEME VOM NETZ ZU TRENNEN

Drei Stufen

STUFE	WORAN ERKENNBAR	WER ENTSCHEIDET	REAKTION INNERHALB VON
Störung			
Notfall			
Krise			

Wenn der normale Weg ausfällt. Legen Sie fest, wie alarmiert wird, wenn Telefonanlage, E-Mail oder das Firmennetz nicht verfügbar sind. In der Praxis ist das eine private Messenger-Gruppe oder eine ausgedruckte Liste im Auto des Geschäftsführers. Beides ist besser als nichts, aber es muss vorher vereinbart sein.

AUSWEICHWEG FÜR DIE ALARMIERUNG

ABSCHNITT 2 VON 10

Die ersten 30 Minuten.

Vier Szenarien, die zusammen den Großteil der Vorfälle abdecken. Gehen Sie die Listen durch und streichen Sie, was bei Ihnen nicht zutrifft. Ergänzen Sie die Namen, die tatsächlich zuständig sind.

A · Verschlüsselung, Erpressung, Befall

Dateien lassen sich nicht öffnen, Dateinamen haben sich geändert, es erscheint eine Forderung.

- ☐ **Betroffene Geräte vom Netz trennen**, Netzkabel ziehen oder WLAN deaktivieren. Nicht herunterfahren und nicht neu starten, der Arbeitsspeicher enthält Hinweise.
- ☐ **Alarmieren** nach Abschnitt 1. Wer das Netz getrennt hat, meldet das sofort weiter.
- ☐ **Datensicherung schreibgeschützt stellen oder physisch trennen**, bevor sie mit verschlüsselt wird. Dieser Schritt ist der wichtigste der ganzen Liste.
- ☐ **Nicht zahlen und nicht antworten**, bevor Geschäftsführung, Versicherung und Dienstleister gesprochen haben.
- ☐ **Beweise sichern**: Bildschirm abfotografieren, Zeitpunkt notieren, Erpresserschreiben nicht löschen.
- ☐ **Strafanzeige vorbereiten**. Zuständig ist die Zentrale Ansprechstelle Cybercrime des jeweiligen Landeskriminalamts.
- ☐ **Prüfen, ob personenbezogene Daten betroffen sind**. Falls ja, läuft die 72-Stunden-Frist nach Abschnitt 8 ab jetzt.

B · Ausfall von Server, Serverraum oder Strom

Zentrale Anwendungen nicht erreichbar, kein Zugriff auf Laufwerke, Ausfall der Klimatisierung.

- ☐ **Ursache grob eingrenzen**: Strom, Netz, Klima, Hardware. Ein Blick in den Raum beantwortet meist mehr als jede Fernanalyse.
- ☐ **Bei Wasser, Rauch oder Hitze den Raum nicht betreten**, sondern Feuerwehr rufen.
- ☐ **Alarmieren** nach Abschnitt 1 und Wiederanlauf-Reihenfolge nach Abschnitt 5 heranziehen.
- ☐ **Notbetrieb anordnen** nach Abschnitt 7, sobald absehbar ist, dass es länger als die vereinbarte Frist dauert.
- ☐ **Mitarbeitende informieren**, was weiterhin funktioniert, nicht nur, was ausgefallen ist.

ABSCHNITT 2 VON 10, FORTSETZUNG

C · Übernommenes Konto

Fremde Nachrichten im eigenen Namen, unbekannte Anmeldungen, Weiterleitungsregeln, die niemand angelegt hat.

- ☐ **Alle Sitzungen des Kontos beenden**, nicht nur das Passwort ändern. Ein bestehendes Anmeldetoken überlebt einen Passwortwechsel.
- ☐ **Passwort ändern und zweiten Faktor neu einrichten.**
- ☐ **Weiterleitungs- und Posteingangsregeln prüfen.** Angreifer legen dort Regeln an, um Antworten umzuleiten. Das ist der häufigste übersehene Punkt.
- ☐ **Prüfen, was versendet wurde** und wer geantwortet hat. Betroffene Empfänger auf einem anderen Weg warnen, nicht per E-Mail aus demselben Postfach.
- ☐ **Bei Zahlungsaufforderungen:** Buchhaltung und Bank sofort informieren. Eine Rechnung mit geänderter Bankverbindung ist das eigentliche Ziel dieser Angriffe.
- ☐ **Prüfen, ob personenbezogene Daten abgeflossen sind**, siehe Abschnitt 8.

D · Ausfall von Internet, Telefonie oder einem Cloud-Dienst

Keine Verbindung nach außen, Microsoft 365 oder eine Fachanwendung nicht erreichbar.

- ☐ **Prüfen, ob der Ausfall beim Anbieter liegt.** Statusseite des Anbieters über eine Mobilfunkverbindung aufrufen, nicht über das eigene Netz.
- ☐ **Bei Anbieterstörung:** Störung melden, Ticketnummer notieren, zugesagte Wiederherstellungszeit erfragen und festhalten.
- ☐ **Ersatzverbindung aktivieren**, Mobilfunk-Router oder Hotspot. Wer ihn holt und wo er liegt, steht unten.
- ☐ **Entscheiden, welche Prozesse auf Papier weiterlaufen** und wer die Nacherfassung macht.
- ☐ **Kunden aktiv informieren**, bevor sie anrufen, siehe Abschnitt 8.

ERSATZVERBINDUNG LIEGT BEI

AUFBEWAHRUNGORT

Eigenes Szenario ergänzen. Wenn Ihr Betrieb von einer Maschinensteuerung, einem Warenwirtschaftssystem oder einer einzelnen Fachanwendung abhängt, gehört dafür ein eigenes Blatt dazu. Fragen Sie sich: welcher Ausfall würde uns am meisten kosten, und steht er in dieser Liste?

UNSER FÜNFTE SZENARIO

ABSCHNITT 3 VON 10

Kritische Prozesse und ihre Fristen.

Welcher Geschäftsprozess verträgt wie viel Stillstand, und was kostet eine Stunde davon. Aus diesen Zahlen leitet sich jede weitere Entscheidung ab, auch die über Ihr Budget.

Diesen Abschnitt füllt nicht die IT aus, sondern die Geschäftsführung zusammen mit den Fachbereichen. Die IT kann sagen, wie lange eine Wiederherstellung dauert. Ob vier Stunden Stillstand hinnehmbar sind, ist eine kaufmännische Frage.

PROZESS	VERANTWORTLICH	VERTRÄGT STILLSTAND VON	KOSTET JE STUNDE ETWA	HÄNGT AB VON
1				
2				
3				
4				
5				
6				
7				

Wie man die Stillstandszeit schätzt

Fragen Sie nicht, wie lange etwas fehlen darf. Fragen Sie: ab wann rufen Kunden an, ab wann können wir nicht mehr liefern, ab wann wird eine Frist gegenüber Behörden oder Auftraggebern verletzt. Der kleinste dieser drei Werte ist die Antwort.

Wie man die Kosten schätzt

Personalkosten der Menschen, die nicht arbeiten können, plus entgangener Umsatz, plus Nacharbeit. Die Nacharbeit wird fast immer vergessen und ist bei Papierbetrieb der größte Posten. Eine grobe Zahl genügt, sie muss nur die Reihenfolge richtig abbilden.

DER PROZESS, BEI DEM WIR UNS AM WENIGSTEN SICHER SIND, UND WARUM

ABSCHNITT 4 VON 10

Abhängigkeiten.

Welche Anwendung braucht welchen Server, welche Datenbank, welche Schnittstelle, welchen externen Dienst. Hier zeigt sich regelmäßig, dass eine Nebensache einen Kernprozess blockiert.

ANWENDUNG ODER DIENST	LÄUFT AUF	BRAUCHT ZWINGEND	LIZENZ ODER ZUGANG BEI	AUSFALL MERKT ZUERST
1				
2				
3				
4				
5				
6				
7				
8				
9				

Die drei Abhängigkeiten, die am häufigsten fehlen. Ein Lizenzserver, der still im Keller läuft und ohne den eine Fachanwendung nach 30 Tagen stehenbleibt. Ein Zertifikat mit Ablaufdatum, das niemand im Kalender hat. Und ein einzelner Mensch, der als einziger weiß, wie ein bestimmter Ablauf funktioniert. Der letzte Punkt ist technisch keine Abhängigkeit, fällt im Notfall aber genauso aus.

WISSEN, DAS NUR EINE PERSON HAT

WER SOLL ES ZUSÄTZLICH KENNEN, BIS WANN

ABSCHNITT 5 VON 10

Wiederaufbau-Reihenfolge.

Was kommt zuerst hoch. Ohne festgelegte Reihenfolge wird im Ernstfall das Lauteste zuerst bearbeitet, nicht das Wichtigste.

Die Reihenfolge ergibt sich aus Abschnitt 3 und 4: erst die Grundlagen, auf denen alles aufsetzt, dann die Prozesse mit der kürzesten vertraglichen Stillstandszeit. Die Spalte rechts bleibt im Normalfall leer und wird im Ereignisfall ausgefüllt.

SYSTEM ODER DIENST	WER MACHT DAS	DAUERT ETWA	VORAUSSETZUNG	FERTIG UM
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				

Erst Grundlagen, dann Anwendungen

Eine brauchbare Reihenfolge beginnt fast immer gleich: Strom, Netz, Namensauflösung und Verzeichnisdienst, Virenschutz, dann Dateidienste, dann Fachanwendungen, zuletzt Nebensysteme. Wer mit der Fachanwendung anfängt, fängt zweimal an.

Teilbetrieb ist erlaubt

Es muss nicht alles gleichzeitig laufen. Legen Sie fest, bei welchem Stand Sie den Betrieb wieder aufnehmen, auch wenn noch nicht alles verfügbar ist. Diese Entscheidung vorab zu treffen spart im Ernstfall eine Stunde Diskussion.

AB DIESEM STAND NEHMEN WIR DEN BETRIEB WIEDER AUF

ABSCHNITT 6 VON 10

Backup und Rücksicherung.

Wo die Sicherungen liegen, wer daran kommt, und wie lange eine Rücksicherung tatsächlich dauert. Nicht laut Datenblatt, sondern gemessen.

WAS WIRD GESICHERT	WOHIN	WIE OFT	AUFBEWAHRUNG	VOM NETZ GETRENNT
1				
2				
3				
4				
5				
6				

Gemessene Wiederherstellung

Nur Zeiten eintragen, die Sie gestoppt haben. Ein ungetesteter Wert ist eine Vermutung und im Ernstfall regelmäßig um den Faktor drei zu optimistisch.

WIEDERHERSTELLUNG VON	GEMESSEN AM	HAT GEDAUERT	WER HAT ES GEMACHT	ANMERKUNG

Die Frage, an der es hängt. Kann Ihre Sicherung von jemandem erreicht werden, der Administratorrechte in Ihrem Netz hat? Wenn die Antwort ja oder unklar lautet, haben Sie im Ernstfall keine Sicherung. Mindestens eine Kopie gehört auf einen Speicher, der nicht dauerhaft erreichbar ist, oder in einen Speicher, der nachträglich nicht verändert werden kann.

WER KANN EINE RÜCKSICHERUNG AUSLÖSEN	ZUGANGSDATEN DAZU LIEGEN	NÄCHSTER TESTTERMIN

ABSCHNITT 7 VON 10

Ausweicharbeitsplätze.

Von wo arbeiten die Menschen, wenn das Gebäude nicht nutzbar ist. Homeoffice trägt einen Teil, aber nicht jeden Prozess.

Der blinde Fleck. Dieser Abschnitt fehlt in fast allen Notfallhandbüchern, auch in den gut gemachten. Sie beantworten lückenlos, wie die IT wiederkommt, und keines beantwortet, wo die Belegschaft in der Zwischenzeit sitzt. Bei einem Wasserschaden, einem Brand im Nachbargebäude oder einer behördlichen Sperrung ist die IT unversehrt und trotzdem steht der Betrieb.

PROZESS	MINDESTBESETZUNG	ARBEITET DANN VON	BRAUCHT DORT	GEPRÜFT AM
1				
2				
3				
4				
5				
6				

Was einen Platz arbeitsfähig macht

Ein Schreibtisch ist kein Arbeitsplatz. Prüfen Sie je Prozess, was tatsächlich gebraucht wird, und streichen Sie, was nicht zutrifft.

- | | |
|--|--|
| ☐ Gerät mit den richtigen Anwendungen, nicht nur ein Browser | ☐ Zugriff auf Unterlagen, die bisher nur im Schrank liegen |
| ☐ Zugang zum Firmennetz, auch wenn der Standort nicht erreichbar ist | ☐ Ein Raum, in dem vertraulich telefoniert werden kann |
| ☐ Telefonie unter der gewohnten Rufnummer, nicht unter einer privaten | ☐ Ein zweiter Faktor, der nicht am Firmenhandy im gesperren Gebäude hängt |
| ☐ Drucker oder Scanner, falls der Prozess Papier braucht | ☐ Jemand, der entscheidet, wer zuerst umzieht |

AUSWEICHSTANDORT, ADRESSE

PLÄTZE DORT / ZULETZT TATSÄCHLICH GENUTZT AM

ABSCHNITT 8 VON 10

Kommunikation nach außen und Meldefristen.

Wer spricht mit Kunden, Lieferanten, Behörden und Presse. Und welche Uhr läuft ab dem Moment, in dem Sie Kenntnis erlangen.

ZIELGRUPPE	SPRICHT	VERTRETUNG	AUF WELCHEM WEG	SPÄTESTENS NACH
Mitarbeitende				
Kunden				
Lieferanten				
Behörden				
Presse				

Gesetzliche Fristen, die ab Kenntniserlangung laufen

GILT FÜR	WAS	FRIST	AN WEN
Alle, bei personenbezogenen Daten	Meldung der Datenschutzverletzung	72 Stunden	Zuständige Landesdatenschutzbehörde, Art. 33 DSGVO
Betroffene nach NIS2	Frühwarnung	24 Stunden	BSI, § 32 BSIG
Betroffene nach NIS2	Folgemeldung mit Bewertung	72 Stunden	BSI, § 32 BSIG
Betroffene nach NIS2	Abschlussbericht	1 Monat	BSI, § 32 BSIG

Gelten diese Fristen für uns? Die 72 Stunden nach DSGVO gelten für jeden, sobald personenbezogene Daten betroffen sein könnten, und das sind sie bei einem Verschlüsselungsvorfall fast immer. Die NIS2-Pflichten nach § 32 BSIG gelten seit dem 6. Dezember 2025 und hängen von Sektor und Unternehmensgröße ab. Prüfen Sie das einmal und tragen Sie das Ergebnis unten ein, damit im Ernstfall niemand danach sucht.

Für Banken, Finanzdienstleister und Versicherungen kommen DORA, MaRisk und die aufsichtlichen Anforderungen an die IT hinzu, mit eigenen Fristen und eigenen Nachweispflichten. Dazu gibt es ein Beiblatt zu dieser Vorlage.

UNTERLIEGEN WIR NIS2? ERGEBNIS DER PRÜFUNG, DATUM

CYBERVERSICHERUNG, POLICE UND NOTFALLNUMMER

Die Angaben zu Fristen sind eine Orientierung nach dem Stand von Oktober 2026 und ersetzen keine Rechtsberatung.

ABSCHNITT 9 VON 10

Externe Ansprechpartner.

Mit Vertragsnummer und zugesagter Reaktionszeit. Eine Telefonnummer ohne Vertragsnummer kostet im Ernstfall zehn Minuten in der Warteschleife.

WOFÜR	FIRMA	NUMMER, RUND UM DIE UHR	VERTRAGS- ODER KUNDENNR.	REAKTION IN
IT-Dienstleister				
Internetanschluss				
Telefonie				
Fachanwendung				
Datensicherung				
Hardware-Hersteller				
Cyberversicherung				
Datenrettung				
Datenschutzbeauftragter				
Polizei, Cybercrime-Stelle				
Elektriker, Schlüsseldienst				

Einmal anrufen und prüfen. Die Notfallnummer eines Dienstleisters ist überraschend oft eine Nummer, die außerhalb der Geschäftszeiten auf einen Anrufbeantworter läuft. Das sollten Sie wissen, bevor Sie es um zwei Uhr nachts herausfinden. Notieren Sie das Ergebnis in der letzten Spalte, nicht die Zusage aus dem Vertrag.

ABSCHNITT 10 VON 10

Nachbereitung.

Was ist passiert, was hat gefehlt, was wird geändert. Ohne diesen Teil wiederholt sich derselbe Vorfall.

Vorfallprotokoll, im Ereignisfall ausfüllen

Mitschreiben, solange es passiert, nicht danach aus der Erinnerung. Diese Zeilen sind später die Grundlage für Versicherung, Behörden und die eigene Bewertung.

UHRZEIT	WAS WURDE BEOBACHTET ODER ENTSCHIEDEN	VON WEM

Auswertung, innerhalb von zwei Wochen

WAS HAT FUNKTIONIERT	WAS WIRD GEÄNDERT, VON WEM, BIS WANN
WAS HAT GEFEHLT	ERLEDIGT AM

Die Auswertung ist keine Schuldzuweisung. Sobald sie als solche verstanden wird, melden Menschen beim nächsten Mal später, und das kostet mehr als jeder Fehler, den sie gemacht haben.

NACHWEISE

Übungsnachweis und Prüfprotokoll.

Der Test zeigt mehr als das Dokument. Ein Handbuch, das nie ausprobiert wurde, beschreibt einen Ablauf, von dem niemand weiß, ob er funktioniert.

Drei Stufen, aufsteigend im Aufwand

Durchsprechen

Eine Stunde am Tisch, ein Szenario vorgelesen, alle sagen, was sie tun würden. Findet die meisten Lücken bei geringstem Aufwand.

Teilweise technisch

Eine Rücksicherung tatsächlich durchführen und die Zeit stoppen. Oder einen Ausweicharbeitsplatz einen Tag wirklich nutzen.

Vollständig

Angekündigter Ausfall eines Systems im laufenden Betrieb. Nur sinnvoll, wenn die beiden ersten Stufen sauber laufen.

DATUM	WAS WURDE GEÜBT	STUFE	TEILNEHMENDE	ERGEBNIS, KURZ

Dokumentenlenkung

Wer dieses Handbuch pflegt, wann es geprüft wurde, und welche Ausfertigungen im Umlauf sind. Veraltete Kontaktdaten sind der häufigste Grund, warum ein vorhandenes Handbuch im Ernstfall nicht trägt.

VERSION	STAND	GEÄNDERT WURDE	GEPRÜFT VON	ALTE AUSDRUCKE VERNICHTET

PRÜFTURNUS, EMPFOHLEN JÄHRLICH UND NACH JEDEM VORFALL

VERANTWORTLICH FÜR DIE PFLEGE

ZUM SCHLUSS

Was dieser Vorlage noch fehlt.

Offen gesagt: das Wichtigste. Diese sechzehn Seiten sind ein Gerüst. Was daraus ein belastbares Handbuch macht, sind Ihre Zahlen, Ihre Namen und ein Test.

Die drei Stellen, an denen es in der Praxis hängt

- ☐ **Abschnitt 3 bleibt leer.** Die vertraglichen Stillstandszeiten zu benennen, ist eine unangenehme Entscheidung, und sie lässt sich nicht an die IT delegieren. Ohne diese Zahlen ist die Reihenfolge in Abschnitt 5 geraten.
- ☐ **Die gemessenen Zeiten in Abschnitt 6 fehlen.** Fast alle Betriebe tragen hier den Wert aus dem Angebot ein. Eine einzige echte Rücksicherung mit Stoppuhr bringt mehr als dieses ganze Dokument.
- ☐ **Es wird nie geübt.** Ein Handbuch im Ordner erzeugt ein Gefühl von Sicherheit, das die erste Stunde eines echten Vorfalls nicht überlebt.

Wenn Sie dabei Unterstützung wollen

Wir bauen solche Handbücher mit Betrieben im Rhein-Main-Gebiet auf, in der Regel in zwei Terminen: einer für die Prozesse und Fristen, einer für den Test. Das geht auch, wenn Ihre IT bei jemand anderem liegt.

Bei den Ausweicharbeitsplätzen aus Abschnitt 7 können wir mehr als beraten: wir halten an drei geografisch getrennten Standorten vorbereitete Plätze bereit, die im Ernstfall sofort nutzbar sind.

CentricCom AG

Konrad-Adenauer-Allee 1 bis 11
61118 Bad Vilbel bei Frankfurt

+49 69 4015000-33

Montag bis Freitag, 7 bis 17 Uhr

centriccom.de/notfallarbeitsplaetze.html

Woher die Angaben stammen

Die Gliederung folgt BSI-Standard 200-4, Kapitel 6.4, 6.9 und 6.10, gekürzt auf den Umfang mittelständischer Betriebe. Die Meldefristen stammen aus Art. 33 DSGVO und § 32 BSIg in der seit dem 6. Dezember 2025 geltenden Fassung. Das Bundesamt für Sicherheit in der Informationstechnik stellt die amtliche Langfassung und weitere Hilfsmittel kostenlos unter bsi.bund.de bereit. Diese Vorlage darf frei verwendet, ausgedruckt und im eigenen Unternehmen angepasst werden.