NOTFALL-KIT

Cyberangriff & IT-Sicherheitsvorfall

Sofortmaßnahmen | Meldepflichten | Vorfallsbericht | Kontakte

Dieses Dokument ausdrucken und griffbereit halten. Im Ernstfall zählt jede Minute.

Kontakt	Telefon / E-Mail
ITSB Notfall-Hotline	089 200 011 380
ITSB WhatsApp (24/7)	+49 155 65830107
ITSB E-Mail	notfall@itsb-deutschland.de
Polizei (Cybercrime)	110 oder zustaendige LKA-Stelle
BSI (KRITIS-Meldung)	0800 274 1000
Datenschutzbehoerde Bayern	www.lda.bayern.de

ITSB Deutschland UG | Tegernseer Landstr. 98, 81539 München | Version 2.0 | 2026

Inhaltsverzeichnis

1. Sofortmassnahmen

DIE ERSTEN 60 MINUTEN SIND ENTSCHEIDEND

- [ ] Ruhe bewahren - keine übereilten Aktionen
- [ ] Betroffene Systeme NICHT ausschalten (Beweissicherung!)
- [ ] Betroffene Systeme vom Netzwerk isolieren (Kabel ziehen, WLAN aus)
- [ ] IT-Sicherheitsverantwortlichen informieren
- [ ] Geschäftsführung informieren
- [ ] Zeitstempel und erste Beobachtungen dokumentieren
- [ ] Screenshots von Fehlermeldungen / Erpresserschreiben machen
- [ ] Keine Lösegeldforderungen bezahlen
- [ ] Passwörter für alle Admin-Konten SOFORT ändern
- [ ] Prüfen: Welche Systeme sind betroffen?
- [ ] ITSB Notfall-Hotline anrufen: 089 200 011 380

2. Analyse & Eindämmung (Stunde 1-4)

- [ ] Art des Angriffs identifizieren (Ransomware, Phishing, DDoS, Insider)
- [ ] Ausmaß des Schadens abschätzen
- [ ] Betroffene Daten identifizieren (personenbezogene Daten?)
- [ ] Backup-Status prüfen (sind Backups sauber und offline?)
- [ ] Forensische Sicherung der betroffenen Systeme
- [ ] Externe IT-Sicherheitsexperten hinzuziehen (ITSB)
- [ ] Kommunikationskanal fuer Krisenstab einrichten
- [ ] Mitarbeitende informieren (was dürfen sie, was nicht)

3. Meldepflichten & Fristen

Meldung	An wen	Frist	Wann
DSGVO Art. 33	Datenschutz-behörde	72 Stunden	Personenbezogene Daten betroffen
DSGVO Art. 34	Betroffene Personen	Unverzüglich	Hohes Risiko fuer Betroffene
NIS2 Frühwarnung	BSI	24 Stunden	NIS2-betroffene Unternehmen
NIS2 Detail	BSI	72 Stunden	Detaillierter Bericht

Meldung	An wen	Frist	Wann
NIS2 Abschluss	BSI	1 Monat	Finaler Bericht
Cyberversicherung	Versicherer	Sofort (Police!)	Frist beachten!
Strafanzeige	Polizei / LKA	Empfohlen: sofort	Bei Straftaten

Wichtig: Bei Versäumnis der DSGVO-Meldefrist drohen Bußgelder bis zu 10 Mio. EUR.

4. Wiederherstellung

- ■ Systeme aus sauberem Backup wiederherstellen
- ■ Sicherheitslücke identifizieren und schliessen
- ■ Alle Passwörter zurücksetzen (ALLE Benutzer)
- ■ MFA fuer alle Konten aktivieren
- ■ Systeme schrittweise wieder ans Netz nehmen
- ■ Monitoring verstärken (mind. 4 Wochen)
- ■ Funktionstest aller wiederhergestellten Systeme
- ■ Externe Kommunikation vorbereiten (Kunden, Partner)

5. Nachbereitung & Lessons Learned

- ■ Detaillierten Vorfallsbericht erstellen (siehe Vorlage)
- ■ Lessons Learned Workshop mit allen Beteiligten
- ■ Sicherheitsmaßnahmen basierend auf Erkenntnissen anpassen
- ■ Mitarbeiterschulung / Awareness-Training durchführen
- ■ Notfallpläne aktualisieren
- ■ Managed Security Service evaluieren (ITSB)
- ■ Nächsten Audit-Termin vereinbaren
- ■ Cyberversicherung prüfen / anpassen

6. Vorfallsbericht - Vorlage

Diese Vorlage ausdrucken oder digital ausfüllen.

Datum des Vorfalls: _____

Uhrzeit der Entdeckung: _____

Entdeckt durch: _____

Art des Vorfalls:

[ ] Ransomware [ ] Phishing [ ] DDoS [ ] Datenleck [ ] Insider [ ] Sonstiges: _____

Betroffene Systeme:

_____

_____

Betroffene Daten:

[ ] Personenbezogene Daten [ ] Finanzdaten [ ] Geschäftsgeheimnisse [ ] Kundendaten

Anzahl betroffener Datensätze (geschätzt): _____

6. Vorfallsbericht - Vorlage (Fortsetzung)

Erste Maßnahmen ergriffen:

_____

_____

Ursache (sofern bekannt):

_____

Meldungen erfolgt:

[ ] Datenschutzbehörde (Datum: _____) [ ] BSI (Datum: _____)

[ ] Polizei (Datum: _____) [ ] Versicherung (Datum: _____)

[ ] Betroffene Personen (Datum: _____)

Externe Unterstützung: _____

Geschätzter Schaden: _____

Status: [ ] Offen [ ] In Bearbeitung [ ] Eingedämmt [ ] Wiederhergestellt [ ] Abgeschlossen

Verantwortlicher: _____

Datum / Unterschrift: _____

7. Wichtige Kontakte

Interne Kontakte (bitte ausfüllen):

Rolle	Name	Telefon	E-Mail
Geschaeftsführung			
IT-Leitung			
IT-Sicherheits-beauftragter			
Datenschutz-beauftragter			

Rolle	Name	Telefon	E-Mail
Ext. IT-Dienstleister			
Cyberversicherung			
Rechtsanwalt			

ITSB Deutschland - Ihr Notfall-Partner:

Dienst	Kontakt
ITSB Notfall-Hotline	089 200 011 380
ITSB WhatsApp (24/7)	+49 155 65830107
ITSB Notfall-E-Mail	notfall@itsb-deutschland.de
ITSB Webseite	itsb-deutschland.de

8. Präventions-Checkliste

Damit es gar nicht erst soweit kommt:

- Backup-Strategie: 3-2-1 Regel (3 Kopien, 2 Medien, 1 offline)
- Backups regelmäßig testen (Recovery-Test mind. quartalsweise)
- Multi-Faktor-Authentifizierung (MFA) für alle Konten
- Patch-Management: Alle Systeme aktuell halten
- Mitarbeiter-Schulungen (Awareness, mind. jährlich)
- Phishing-Simulationen durchführen
- Netzwerksegmentierung implementiert
- Endpoint-Security auf allen Geräten
- Zugriffsrechte nach Least-Privilege-Prinzip
- Notfallplan vorhanden und getestet
- Cyberversicherung abgeschlossen und aktuell
- Externe Sicherheitsüberprüfung (mind. jährlich)
- Incident-Response-Plan dokumentiert
- Logging und Monitoring aktiv
- Managed Security Service evaluiert (ITSB)

ITSB NOTFALL-HOTLINE: 089 200 011 380

notfall@itsb-deutschland.de | WhatsApp: +49 155 65830107

itsb-deutschland.de