Notfallkarte: Die ersten 60 Minuten

Bei einem IT-Sicherheitsvorfall. Ausdrucken und griffbereit halten.

1. **Ruhe bewahren und Krisenstab alarmieren**
   Rollen besetzen, Vertretungen nutzen. Entscheidungen trifft die Leitung des Krisenstabs.
2. **Betroffene Systeme vom Netz trennen**
   Möglichst nicht sofort ausschalten, damit Spuren erhalten bleiben. Keine Aufräumversuche.
3. **Backups schützen**
   Sicherungen vom Netz trennen, bevor sie erreicht werden.
4. **Alles dokumentieren**
   Zeitstrahl führen: Wer hat wann was getan? Fotos von Meldungen, keine Verschleierung.
5. **Meldepflichten prüfen**
   Fristen laufen ab Kenntnis des Vorfalls. Siehe Kasten unten.
6. **Experten holen**
   Forensik und Incident-Response-Dienstleister früh einbinden, ebenso Versicherung und Datenschutz.

Meldefristen nach NIS2 (falls betroffen)

24 Stunden	Frühwarnung an das BSI
72 Stunden	Meldung mit erster Bewertung (bei Personendaten zusätzlich Datenschutzbehörde)
1 Monat	Abschlussbericht

Wichtige Kontakte

Leitung Krisenstab _____

IT-Leitung / Administration _____

Datenschutz _____

Geschäftsleitung _____

Incident-Response-Dienstleister _____

Cyberversicherung (Schadensmeldung) _____

Polizei / Zentrale Ansprechstelle Cybercrime _____

Nicht tun

Nicht sofort alles herunterfahren oder neu installieren. Kein Lösegeld ohne Rücksprache mit Krisenstab, Rechtsberatung und Strafverfolgung. Keine Details öffentlich oder in sozialen Netzwerken teilen, bevor die Kommunikation abgestimmt ist.