Arbeitshilfe 1: Checkliste Ransomware-Notfall	
Aufgabe	✔
Sofortmaßnahmen (erste Stunde)	
Betroffene Systeme isolieren (nicht einfach abschalten!)	◯
Geschäftsführung informieren	◯
IT-Abteilung/Informationssicherheitsbeauftragten informieren	◯
Cyberversicherung kontaktieren (24/7-Hotline)	◯
Datenschutzbeauftragten informieren	◯
Krisenmanager konkret benennen	◯
Entscheidungsbefugnisse klarstellen	◯
IT-Forensiker beauftragen (über Versicherung oder direkt)	◯
Prüfen, ob Back-ups betroffen/verschlüsselt sind	◯
Keine Zahlung ohne Forensik-Ergebnis!	◯
Meldung (binnen 72 Stunden)	
Je nach Unternehmen: Meldung an BSI nach BSIG (Frist: 24 Stunden)	◯
Prüfen, ob meldepflichtige Datenschutzverletzung nach Art. 33 DSGVO vorliegt	◯
Vormeldung an Aufsichtsbehörde (auch wenn Details fehlen!)	◯
Notfallteam zusammenstellen (GF, IT, DSB, Rechtsabteilung)	◯
Kommunikationsstrategie festlegen	◯
Aufarbeitung (erste Woche)	
Forensik-Ergebnisse abwarten	◯
Beweise sichern (Logfiles, Speicherabbilder, Zeitstempel)	◯
Umfang der Kompromittierung feststellen	◯
Betroffene Personen identifizieren	◯
Risikobewertung durchführen	◯
Kommunikation (laufend)	
Nachmeldung an Aufsichtsbehörde mit Details	◯
Information an Betroffene (falls hohes Risiko)	◯
Regelmäßige Updates an Behörden	◯
Dokumentation aller Schritte	◯
Entscheidungsdokumentation (warum gemeldet/informiert/ Zahlung verweigert)	◯
Nachbesserung (erste 60 Tage)	
Schwachstelle schließen	◯
TOM nachbessern	◯
Mitarbeiter schulen	◯
Maßnahmenplan vollständig umsetzen	◯
Dokumentation vervollständigen	◯