Incident-Logbuch & Zeitleiste

Das Logbuch ist das erste Dokument, das der IR-Leiter aufschlägt: Es rekonstruiert, **was wann von wem entdeckt, entschieden und getan wurde** – Grundlage für Forensik, Versicherung, die 72-Stunden-Meldung nach Art. 33 DSGVO und spätere Gerichtsverwertbarkeit. Ohne Logbuch widersprechen sich nach 48 Stunden die Erinnerungen aller Beteiligten.

Warum dieses Dokument?

Forensik, Versicherung und Behörden fragen zuerst nach der Zeitleiste. Und: Wer dokumentieren muss, handelt überlegter – das Logbuch diszipliniert in der hektischsten Phase.

Wann brauchen Sie es?

Ab der ersten Minute jedes Vorfalls – Eintrag Nr. 1 ist die Entdeckung. Danach jede Beobachtung, Maßnahme, Entscheidung und externe Kommunikation, fortlaufend nummeriert.

Wo aufbewahren?

Mehrere Blanko-Blätter ausgedruckt im Notfallordner – mit Klemmbrett und Kugelschreiber. Handschriftlich ist völlig okay; digital ist im Ransomware-Fall oft nichts erreichbar.

So bleibt die Zeitleiste verwertbar

1. **Eine Referenzuhr** – alle Uhrzeiten von derselben Uhr, Zeitzone notieren
2. **Sofort eintragen** – nicht abends aus dem Gedächtnis rekonstruieren
3. **Beweis referenzieren** – Foto-Nr., Datei, Screenshot – und wo es abgelegt ist
4. **Blatt abschließen** – Schreiber + Blatt-Nr. eintragen, nächstes Blatt beginnen

Grundregel: Lieber zu viel als zu wenig – auch „nichts Neues seit 14:00“ ist ein Eintrag. Streichungen nur durchstreichen, nie unkenntlich machen.

So sieht ein ausgefülltes Logblatt aus

BEISPIEL – Muster Maschinenbau GmbH (fiktiv) · Incident „MM-2026-001 Ransomware“, Blatt 1, Schreiber: T. Berger

Nr.	Zeit (MESZ)	Ereignis / Maßnahme	Typ	System	Von / Entschieden von
1	05.06. 04:15	Ransomnote „readme.txt“ auf TS-02 entdeckt	Beob.	TS-02	M. Yilmaz
2	05.06. 04:22	TS-02 vom Netz getrennt (Kabel), Foto IMG_0041	Maßn.	TS-02	M. Yilmaz
3	05.06. 04:48	Entscheidung: Internet-Breakout getrennt	Entsch.	FW-01	T. Berger / GF telefonisch
4	05.06. 05:10	Cyber-Versicherung Hotline informiert, Vorgangs-Nr. 88-1234	Komm.	–	K. Sommer

⚠ **Handschriftlich ist okay – lieber zu viel als zu wenig.** Uhrzeiten von EINER Referenzuhr nehmen (z. B. ein bestimmtes Mobiltelefon) und die Zeitzone auf jedem Blatt vermerken. Abweichende Systemuhren sind einer der häufigsten Gründe, warum Zeitleisten vor Versicherung und Gericht wackeln.

Halbjährliche Prüfung: ☐ genügend Blanko-Blätter im Ordner ☐ Klemmbrett + Stift dabei ☐ Referenzuhr festgelegt
Geprüft am: _____ von: _____

Im Ernstfall – Argos IR-Hotline 24/7
+49 89 45 24 24-112

UNTERNEHMEN	STAND / VERSION	VERANTWORTLICH	ORT DER OFFLINE-KOPIE	NÄCHSTE PRÜFUNG

INCIDENT-BEZEICHNUNG	INCIDENT-NR.	BLATT-NR.	SCHREIBER DES BLATTES	ZEITZONE

LOGBUCH – EIN EINTRAG PRO ZEILE, FORTLAUFEND NUMMERIERT

Nr.	Datum + Uhrzeit	Ereignis / Beobachtung / Maßnahme	Typ	System / Konto	Durchgef. / gemeldet von	Entschieden von	Beweismittel (wo abgelegt?)
			☐ B ☐ M ☐ E ☐ K				
			☐ B ☐ M ☐ E ☐ K				
			☐ B ☐ M ☐ E ☐ K				
			☐ B ☐ M ☐ E ☐ K				
			☐ B ☐ M ☐ E ☐ K				
			☐ B ☐ M ☐ E ☐ K				
			☐ B ☐ M ☐ E ☐ K				
			☐ B ☐ M ☐ E ☐ K				
			☐ B ☐ M ☐ E ☐ K				
			☐ B ☐ M ☐ E ☐ K				

Typ: **B** = Beobachtung · **M** = Maßnahme · **E** = Entscheidung · **K** = Kommunikation extern | Bei Entscheidungen immer „Entschieden von“ ausfüllen.

Im Ernstfall – Argos IR-Hotline 24/7
+49 89 45 24 24-112

INCIDENT-BEZEICHNUNG	INCIDENT-NR.	BLATT-NR.	SCHREIBER DES BLATTES	ZEITZONE

LOGBUCH – EIN EINTRAG PRO ZEILE, FORTLAUFEND NUMMERIERT

Nr.	Datum + Uhrzeit	Ereignis / Beobachtung / Maßnahme	Typ	System / Konto	Durchgef. / gemeldet von	Entschieden von	Beweismittel (wo abgelegt?)
			☐ B ☐ M ☐ E ☐ K				
			☐ B ☐ M ☐ E ☐ K				
			☐ B ☐ M ☐ E ☐ K				
			☐ B ☐ M ☐ E ☐ K				
			☐ B ☐ M ☐ E ☐ K				
			☐ B ☐ M ☐ E ☐ K				
			☐ B ☐ M ☐ E ☐ K				
			☐ B ☐ M ☐ E ☐ K				
			☐ B ☐ M ☐ E ☐ K				
			☐ B ☐ M ☐ E ☐ K				
			☐ B ☐ M ☐ E ☐ K				
			☐ B ☐ M ☐ E ☐ K				

Typ: **B** = Beobachtung · **M** = Maßnahme · **E** = Entscheidung · **K** = Kommunikation extern | Bei Entscheidungen immer „Entschieden von“ ausfüllen.

Im Ernstfall – Argos IR-Hotline 24/7
+49 89 45 24 24-112

INCIDENT-BEZEICHNUNG	INCIDENT-NR.	BLATT-NR.	SCHREIBER DES BLATTES	ZEITZONE

LOGBUCH – EIN EINTRAG PRO ZEILE, FORTLAUFEND NUMMERIERT

Nr.	Datum + Uhrzeit	Ereignis / Beobachtung / Maßnahme	Typ	System / Konto	Durchgef. / gemeldet von	Entschieden von	Beweismittel (wo abgelegt?)
			☐ B ☐ M ☐ E ☐ K				
			☐ B ☐ M ☐ E ☐ K				
			☐ B ☐ M ☐ E ☐ K				
			☐ B ☐ M ☐ E ☐ K				
			☐ B ☐ M ☐ E ☐ K				
			☐ B ☐ M ☐ E ☐ K				
			☐ B ☐ M ☐ E ☐ K				
			☐ B ☐ M ☐ E ☐ K				
			☐ B ☐ M ☐ E ☐ K				
			☐ B ☐ M ☐ E ☐ K				
			☐ B ☐ M ☐ E ☐ K				
			☐ B ☐ M ☐ E ☐ K				

Typ: **B** = Beobachtung · **M** = Maßnahme · **E** = Entscheidung · **K** = Kommunikation extern | Bei Entscheidungen immer „Entschieden von“ ausfüllen.

Im Ernstfall – Argos IR-Hotline 24/7
+49 89 45 24 24-112