Lessons-Learned-Template

1. Vorfallbeschreibung:
- Datum und Uhrzeit des Vorfalls
- Art des Vorfalls (z. B. Datenleck, Malware-Angriff)
- Betroffene Systeme und Daten

2. Reaktionsdetails:
- Maßnahmen, die ergriffen wurden, um den Vorfall zu beheben
- Beteiligte Teams und deren Rollen
- Zeitrahmen der Reaktion

3. Ursachenanalyse:
- Identifizierte Schwachstellen oder Fehler, die zum Vorfall geführt haben
- Externe Faktoren, die den Vorfall beeinflusst haben könnten

4. Ergebnisse:
- Auswirkungen des Vorfalls auf das Unternehmen (finanziell, reputationsmäßig, operationell)
- Erfolgreiche Maßnahmen und Strategien

5. Empfehlungen:
- Verbesserungen für die Sicherheitsinfrastruktur
- Schulungsbedarf für Mitarbeiter
- Änderungen an Prozessen oder Richtlinien

6. Follow-up-Aktionen:
- Geplante Maßnahmen zur Umsetzung der Empfehlungen
- Verantwortliche Personen und Fristen

7. Zusätzliche Anmerkungen:

- Sonstige relevante Informationen oder Beobachtungen