Incident Response (Stand 2026)

Stundensätze (p.P.):

Rolle	Support	Consultant	Expert	Lead
1h (08-18 Uhr)	175 €	275 €	350 €	450 €

- Nachtzuschlag 50% (18:00-08:00 Uhr)
- Wochenend-/Feiertagzuschlag: 100%
- Reisezeit: ½ des Stundensatzes
- Reise- / Materialkosten: Zusätzlich in voller Höhe

Expertenhotline (Stand 2026)

UN-Kategorie	Klein	Mittel	Groß	Sehr groß
Gebühr (pro Monat)	1.200,00 €	1.900,00 €	3.500,00 €	individuell

IT-Forensiker am Telefon

24/7 Erhöhte Erreichbarkeit

1–X Kostenloses Anrufkontingent

Hilfe nach Verfügbarkeit

Kennenlern-Workshop

Präventions-paket

Bevorzugte Behandlung

Jahresgebühr verrechenbar

Für ein Angebot, kommt gerne auf uns zu.

ResponseOne GmbH, Bundesallee 88, 12161 Berlin
+49 (0) 30 86 323 68 0 | info@response.one | www.response.one

ResponseOne

Was gehört zur Incident Response?

Krisen-management

IT-Forensik

Krisen-kommunikation

Notbetrieb

Experten-hotline

IT-Security

Verhandlung / Lösegeldzahlung

IT-Wiederaufbau

Was macht uns aus?

Fokus Mensch

360° Ganzheitlich

Sehr hohe Aufklärungsquote

Vor-Ort-Hilfe

Erfahrung

APT Spezialisierung: staatl. Akteure

Synergie

Flexibel & lösungsorientiert

Checkliste Cyberangriff – Am Beispiel Ransomware

Solltet ihr feststellen, dass einzelne Systeme (Clients oder Server) oder ganze IT-Landschaften von einem Cyberangriff betroffen sind (z.B. Verschlüsselung oder Schadsoftware), leitet bitte umgehend entsprechende Maßnahmen ein. Hier ist der Zeitfaktor sehr entscheidend, da sich der Angriff ggf. noch eindämmen lässt bzw. sich noch Daten retten lassen. Selbstverständlich handelt es sich bei der Checkliste um allgemeine Maßnahmen, die immer an die eigene Situation anzupassen sind.

Maßnahme	Check
1. Verändert nichts auf den Systemen, z.B. keine Dateien löschen und keinen Virenscan durchführen. Soweit möglich, Fotos der Auffälligkeiten machen (z.B. via Handy).	
2. Nicht mit privilegierten / administrativen Konten an betroffenen Systemen anmelden.	
3. Trennt betroffene Systeme vom Netzwerk und schaltet diese schnellstmöglich aus (kein Herunterfahren, sondern Stecker ziehen / hart ausschalten).	
4. Kontaktiert euren Incident Response Dienstleister des Vertrauens. Beispiel: ResponseOne GmbH Hotline: +49 (0)30 86 323 68 68 | notfall@response-one.de	
5. Sichert wichtige Daten für die IT-Forensik, z.B. Logdateien von Firewalls, Domain Controllern, Virenscannern, etc.	
6. Stimmt mit dem Incident Responder weitere Erstmaßnahmen zur Eindämmung / Aufklärung ab.	
7. Bewertet das Ereignis: Ist es eine Störung, ein Notfall oder eine Krise? (Ransomware ist fast immer eine Krise!)	
8. Alarmiert die Geschäftsführung / den Krisenstabsleiter.	
9. Legt einen geeigneten Treffpunkt für den Krisenstab / IT-Stab fest und beruft diesen ein. Treffpunkt lokal oder remote, Uhrzeit?	
10. Legt fest, wer die Alarmierung der einzelnen Stabsmitglieder übernimmt.	
11. Bereitet den Stabsraum vor und prüft, ob alle notwendigen Arbeitsmaterialien vorhanden sind.	

Detektionsphase

Alarmierungsphase

Besprechungsphase

Maßnahme	Check
12. Legt eine Agenda für den Lagevortrag fest oder nutzt folgendes Beispiel: Start erster Lagevortrag durch den Leiter des Krisenstabs.	
a. Erstellt eine Übersicht der bekannten Fakten zum Vorfall, visualisiert die Ausgangslage und beginnt mit einem Protokoll. ▪ Was ist wann passiert? ▪ Welche Auswirkungen hat das Ereignis auf das Unternehmen? ▪ Soweit möglich erstellt eine Lageprognose (Best Case, Worst Case und ggf. Most likely Case)	
b. Erstellt eine Übersicht der bisher ergriffenen Maßnahmen.	
c. Tragt fehlende (relevante) Informationen und Maßnahmen zusammen. Ab der zweiten Stabsrunde: Geht vorab die Maßnahmen der letzten Stabssitzung durch und prüft, ob die Maßnahmen wirksam / erfolgreich waren.	
d. Erteilt weitere Arbeitsaufträge und Maßnahmen. Wer macht was, bis wann und mit welcher Priorität? ▪ zur Aufklärung ▪ zur Eindämmung ▪ zur Kommunikation ▪ zum Aufbau eines Notbetriebes	
13. Prüft, ob weitere Stabsmitglieder, Experten, Datenschutz- oder Strafverfolgungsbehörden benötigt werden oder darüber informiert werden sollten.	
14. Legt eine Krisenmanagement-Strategie fest.	
15. Prüft, welche Kommunikationsstrategie gelten soll und wie die Erstinformation erfolgt (Medium, Botschaft, etc.).	

ResponseOne