

# Incident Response (Stand 2025)

Tagessätze (8h) pro Person:

Rolle	Support	Basic	Expert	Lead
Tag (08-18 Uhr)	1.500,00 €	2.000,00 €	2.500,00 €	3.000,00 €

- Nacht- / Wochenendzuschlag: 50%
- Reisezeit: halber Tagessatz
- Reise- / Materialkosten: Zusätzlich in voller Höhe

# Expertenhotline (Stand 2025)

UN-Kategorie	Klein	Mittel	Groß	Sehr groß
Gebühr (pro Monat)	800,00 €	1.500,00 €	2.500,00 €	individuell



IT-Forensiker  
am Telefon

**24/7**

Erhöhte  
Erreichbarkeit



Kostenloses  
Anrufrkontingent



Hilfe nach  
Verfügbarkeit



Kennenlern-  
Workshop



Präventions-  
paket



Bevorzugte  
Behandlung



Jahresgebühr  
verrechenbar

Für ein Angebot, kommt gerne auf uns zu.



# 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

ResponseOne GmbH, Bundesallee 88, 12161 Berlin

+49 (0) 30 86 323 68 0 | info@response-one.de | www.response-one.de

# 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		Maßnahme	Check	
1. Verändert nichts auf den Systemen, z.B. keine Dateien löschen und keinen Virensan durchführen. Soweit möglich, Fotos der Auffälligkeiten machen (z.B. via Handy).		Detektionsphase	12. Legt eine Agenda für den Lagevortrag fest oder nutzt folgendes Beispiel: Start erster Lagevortrag durch den Leiter des Krisenstabs.		
2. Nicht mit privilegierten / administrativen Konten an betroffenen Systemen anmelden.			Besprechungsphase	a. Erstellt eine Übersicht der bekannten Fakten zum Vorfall, visualisiert die Ausgangslage und beginnt mit einem Protokoll. <ul style="list-style-type: none"> <li>▪ Was ist wann passiert?</li> <li>▪ Welche Auswirkungen hat das Ereignis auf das Unternehmen?</li> <li>▪ Soweit möglich erstellt eine Lageprognose (Best Case, Worst Case und ggf. Most likely Case)</li> </ul>	
3. Trennt betroffene Systeme vom Netzwerk und schaltet diese schnellstmöglich aus (kein Herunterfahren, sondern Stecker ziehen / hart ausschalten).				b. Erstellt eine Übersicht der bisher ergriffenen Maßnahmen.	
4. Kontaktiert euren Incident Response Dienstleister des Vertrauens. Beispiel: ResponseOne GmbH Hotline: +49 (0)30 86 323 68 68   <a href="mailto:notfall@response-one.de">notfall@response-one.de</a>				c. Tragt fehlende (relevante) Informationen und Maßnahmen zusammen. Ab der zweiten Stabsrunde: Geht vorab die Maßnahmen der letzten Stabsitzung durch und prüft, ob die Maßnahmen wirksam / erfolgreich waren.	
5. Sichert wichtige Daten für die IT-Forensik, z.B. Logdateien von Firewalls, Domain Controllern, Virensclannern, etc.				d. Erteilt weitere Arbeitsaufträge und Maßnahmen. Wer macht was, bis wann und mit welcher Priorität? <ul style="list-style-type: none"> <li>▪ zur Aufklärung</li> <li>▪ zur Eindämmung</li> <li>▪ zur Kommunikation</li> <li>▪ zum Aufbau eines Notbetriebes</li> </ul>	
6. Stimmt mit dem Incident Responder weitere Erstmaßnahmen zur Eindämmung / Aufklärung ab.				13. Prüft, ob weitere Stabsmitglieder, Experten, Datenschutz- oder Strafverfolgungsbehörden benötigt werden oder darüber informiert werden sollten.	
7. Bewertet das Ereignis: Ist es eine Störung, ein Notfall oder eine Krise? (Ransomware ist fast immer eine Krise!)				14. Legt eine Krisenmanagement-Strategie fest.	
8. Alarmiert die Geschäftsführung / den Krisenstabsleiter.		Alarmierungsphase		15. Prüft, welche Kommunikationsstrategie gelten soll und wie die Erstinformation erfolgt (Medium, Botschaft, etc.).	
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.					