

# **Leistungsbeschreibung**

## **Incident Response und Forensik Service**

## Inhalt

1	Einführung.....	3
1.1	Unternehmen.....	3
1.2	Hintergrund und Ziele .....	3
2	Überblick über die zu erbringende Leistung .....	4
2.1	Leistungsübersicht .....	4
2.2	Kickoff-Termin (Kickoff-Workshop) .....	5
2.3	Notfallübung .....	5
2.4	Service Level Agreement (SLA) .....	5
3	Retainer-Modell.....	6
4	Abruf der Dienstleistung .....	6
5	Qualifizierung .....	7
5.1	Fachexpertise IT-Forensiker:in .....	7
5.2	Zertifizierung, Testate und Nachweise.....	7
6	Organisatorische und technische Anforderungen in der Informationssicherheit.....	7
7	Datenschutz .....	8

# **1 Einführung**

## **1.1 Unternehmen**

Die Techniker Krankenkasse (TK) ist eine bundesweite Krankenkasse mit rund 9,6 Millionen Mitgliedern und insgesamt rund 12 Millionen Versicherten. Als gesetzliche Krankenversicherung ist die TK eine Körperschaft des öffentlichen Rechts mit Selbstverwaltung. Sie wird von einem hauptamtlichen Vorstand geführt. Circa 15.500 Mitarbeitende betreuen die Versicherten der TK bundesweit an ca. 169 Standorten und in der Unternehmenszentrale (UZ) in Hamburg.

## **1.2 Hintergrund und Ziele**

Die Komplexität von Angriffen auf IT-Systeme steigt kontinuierlich und auch die TK ist dem Risiko ausgesetzt, dass ein solcher Angriff erfolgreich ist. Zur Bewältigung außerordentlicher Bedrohungslagen, vermuteter oder bereits erfolgreicher Angriffe oder Manipulationen auf IT-Systeme bedarf es daher, neben dem Aufbau interner Expertise, der Unterstützung hoch spezialisierter Dienstleister.

Als Orientierung für außerordentliche Bedrohungslagen können grundsätzlich die Risikostufen des Bundesamtes für Sicherheit in der Informationstechnik (BSI), wie sie im Warn- und Informationsdienst (WID) des CERT-Bund beschrieben sind, mit den Einstufungen „Hohes Risiko“ oder „Kritisches Risiko“ als Maßstab betrachtet werden.

Zu diesem Zweck wird ein On Demand Incident Response und Forensik Service gefordert, der nach vereinbarten Service Levels bei der Bewertung und Bewältigung von vermuteten, potenziellen oder konkreten Angriffen auf die TK unterstützt. In Abhängigkeit von der Schwere des Vorfalls ist eine Remote Unterstützung oder vor Ort Präsenz des Dienstleisters erforderlich.

Das Ziel ist, die Auswirkungen auf Geschäftsprozesse durch vermutete oder bereits erfolgte Angriffe auf die IT-Systeme der TK zu minimieren und mögliche Datenabflüsse zu unterbinden. Durch die frühzeitige Erkennung, schnelle Bewertung und gezielte Bewältigung von Bedrohungen soll die Handlungsfähigkeit der TK jederzeit aufrechterhalten und die Auswirkung auf kritische Geschäftsprozesse nachhaltig reduziert werden.

Der On Demand Incident Response und Forensik Service stellt sicher, dass im Ereignisfall kurzfristig qualifizierte Forensiker:innen zur Verfügung stehen, die Angriffe strukturiert analysieren, geeignete Gegenmaßnahmen einleiten sowie eine gerichtsfeste Beweissicherung durchführen. Dabei umfasst der Leistungsumfang nicht nur die technische Analyse, sondern auch eine lückenlose Dokumentation des Vorfalls.

In ihrer Nachhaltigkeitsstrategie hat die TK sich die Ziele gesetzt, in ihrem eigenen Handeln und wesentlichen vor- und nachgelagerten Aktivitäten CO<sub>2</sub>-neutral zu werden sowie Nachhaltigkeit in den Einkaufsprozess zu integrieren. Daher ist der TK wichtig, auch bei der Gestaltung und Beschaffung von (digitalen) Produkten und Leistungen ein Augenmerk auf ökologische und soziale Auswirkungen zu legen.

## **2 Überblick über die zu erbringende Leistung**

### **2.1 Leistungsübersicht**

Die Leistung des Auftragnehmers (AN) besteht in der Bereitstellung der Dienstleistung von On Demand Incident Response und Forensik Services.

Im Rahmen der Dienstleistung MÜSSEN u. a. folgenden Leistungen vom AN erbracht werden:

1. Suche nach Indikatoren für einen vermuteten oder erfolgreichen Angriff.  
Unterstützung bei der Suche nach Indicators of Compromise (IoC), z. B. verdächtige Log-Einträge oder ungewöhnliche Netzwerk-Traffic-Muster.
2. Bestimmung des Angriffs-Umfangs.  
Ermittlung des Ausmaßes eines potenziellen, vermuteten oder erfolgten Angriffs, Bewertung des potenziellen Schadens.
3. Analyse der Angriffsvektoren.  
Aufklärung, über welche Zugangskanäle der Angreifer in die IT-Umgebung eingedrungen ist (Ursachenanalyse).
4. Analyse von Malware.  
Untersuchung und Klassifizierung von gefundenen Schadprogrammen, Erarbeitung von Entfernuungsmaßnahmen.
5. Aussperrung des Angreifers.  
Unterstützung bei sofortigen Maßnahmen zur Sperrung kompromittierter Accounts, Trennung betroffener Systeme. Unterstützung bei sofortigen Maßnahmen zur Eindämmung eines eingetretenen Sicherheitsvorfalls.
6. Verhinderung eines erneuten Angriffs.  
Unterstützung bei der Umsetzung zusätzlicher Schutzmaßnahmen, um ein Wiederauftreten zu verhindern.
7. Bereinigung kompromittierter Systeme.  
Systematische Säuberung betroffener Clients, Server und Netzwerkinfrastruktur, Wiederherstellung aus gesicherten Snapshots und Validierung der Funktionsfähigkeit.
8. Gerichtsfeste forensische Sicherung und Auswertung.  
Digitale Forensik zur Erstellung einer revisionssicheren, gerichtsfesten Beweissicherung und Auswertung der gesicherten Spuren.
9. Unterstützung bei der Wiederherstellung.  
Unterstützung bei Sofortmaßnahmen, welche den IT-Betrieb wiederherstellen.
10. Dokumentation und Nachbereitung.  
Bereitstellung der fallbezogenen Dokumentation und Unterstützung der Nachbereitung.
11. Führen von Verhandlungen.  
Sollte dies im Falle eines Vorfalls notwendig sein, bindet der AN ein/e Verhandlungsführer:in ein.

Der Support MUSS in deutscher Sprache erfolgen. Dies inkludiert den Schriftverkehr und die mündliche Kommunikation. Zudem SOLL die forensische Auswertung in Deutschland stattfinden. Außerdem SOLL der AN über ein portables oder mobiles Labor für die forensischen Analysen (z.B. Forensik-Koffer oder Forensik-Van) verfügen.

Unterstützungsleistungen MÜSSEN mit fundierter Expertise durch ein Threat Intelligence Team des AN ausgeführt werden. Entsprechende Fähigkeiten sind daher mindestens für Windows Clients, Windows Server, MacOS, Microsoft Active-Directory, Exchange, SharePoint,

MS SQL, Oracle (Datenbanken), Webtechnologien, Linux, SAP, Netzwerkinfrastruktur, gängige Virtualisierungsmaschinen und Microsoft 365 Cloud-Dienste für den kurzfristigen Einsatz für die TK vorzuhalten. Der Einsatz KANN in Abhängigkeit von der Schwere des Vorfalls vor Ort bei der TK erforderlich sein. Die Notwendigkeit eines Vor-Ort-Einsatzes wird durch die TK bestimmt. Der AN bietet mindestens 2 Termine pro Jahr zum Austausch mit der TK an. Ziel der Termine ist es, die Aktualität und Angemessenheit der etablierten Prozesse und Maßnahmen zu evaluieren und ggf. anzupassen. Der AN SOLL eine IT-Infrastrukturanalyse in Abstimmung mit der TK vornehmen, um Maßnahmenempfehlungen abzuleiten und die TK bei der Umsetzung dieser unterstützen. Zusätzlich SOLL der AN bei nicht genutzten Personentagen ein optionales Angebot zur Verfügung, das die TK für präventive Cyber-Security-Übungen nutzen kann (z.B. Table Top Exercises, Threat Hunting).

Eventuell anfallende Lizenzkosten der durch den AN im Rahmen der Leistungserbringung eingesetzten Produkte trägt der AN.

## **2.2 Kickoff-Termin (Kickoff-Workshop)**

Unverzüglich, spätestens jedoch zwei Wochen nach Beginn der Vertragslaufzeit führt der AN mit der TK einen ganztägigen (ca. 8 Stunden) Kickoff-Termin in der Unternehmenszentrale der TK vor Ort durch. Der konkrete Zeitpunkt des Termins wird zwischen der TK und dem AN einvernehmlich abgestimmt. An dem Kickoff-Termin werden mindestens die projektbeteiligten TK-Mitarbeitenden aus den Fachabteilungen teilnehmen. Von Seiten des AN haben an diesem Termin mindestens ein technischer und fachlicher Ansprechpartner teilzunehmen. Der AN MUSS ein Konzept zum Kick-Off-Workshop erstellen und diesen vorbereiten sowie moderieren.

In diesem Workshop werden relevante Schnittstellen zwischen, den bei der TK vorhandenen, Systemen analysiert und definiert. Außerdem werden TK interne Prozesse mit Bezug auf das Incident Management sowie die Forensik mit der Arbeitsweise des AN abgestimmt. Für den weiteren Verlauf der Kommunikation ist von dem AN ein Ansprechpartner zu nennen. Sofern aus Sicht des AN weitere Themen im Kickoff-Termin behandelt werden sollen, hat der AN der TK dies im Vorfeld des Kickoff-Termins mitzuteilen. Zudem werden Eskalationsstufen, Ansprechpartner und Kontaktdaten beider Parteien in diesem Workshop festgelegt.

Im Anschluss an den Kickoff-Termin erstellt der AN ein Protokoll über die Ergebnisse des Kick-off-Termins in Textform und sendet dieses Protokoll per E-Mail innerhalb von drei Werktagen nach Ende des Termins der TK zur Abstimmung zu.

## **2.3 Notfallübung**

Der AN MUSS einmal jährlich eine vollumfängliche Notfallübung in den Räumlichkeiten der Unternehmenszentrale (UZ) der TK in Hamburg durchführen. Die Übung umfasst u. a. die Simulation eines gravierenden Sicherheitsvorfalls, die Koordination aller relevanten Stakeholder sowie die anschließende Auswertung und Ableitung konkreter Verbesserungs- und Präventionsmaßnahmen.

## **2.4 Service Level Agreement (SLA)**

Es müssen folgende SLAs eingehalten werden:

- Der Service MUSS kontinuierlich (24 Stunden am Tag, 7 Tage die Woche, 365 Tage im Jahr) zur Verfügung stehen.
- Die Reaktionszeit nach einer initialen Meldung darf maximal 4 Stunden betragen.
- Bei von der TK angeforderter Vor-Ort-Unterstützung MUSS sich mindestens ein IT-Forensiker innerhalb von 24 Stunden an dem betroffenen TK-Standort befinden.

Der AN SOLL innerhalb von 8 Stunden mindestens einen/eine Forensiker:in in der Unternehmenszentrale der TK in Hamburg bereitstellen.

### **3 Retainer-Modell**

Zur Sicherstellung einer schnellen und effektiven Reaktion auf IT-Sicherheitsvorfälle MUSS der AN seine Leistungen im Rahmen eines Retainer-Modells anbieten. Ziel ist es, im Ereignisfall ohne zeitliche Verzögerung handlungsfähig zu sein und qualifizierte Unterstützung unmittelbar bereitstellen zu können.

Die tatsächlich benötigten Unterstützungsleistungen werden anlassbezogen und nach Bedarf durch die TK abgerufen. Dies umfasst alle Leistungen nach Kapitel 2. Schätzungsweise werden über die Vertragslaufzeit ca. 20 Personentage abgerufen, maximal 60 Personentage. Eine Abnahme-/Abrufverpflichtung besteht nicht.

Die Abrechnung erfolgt auf Basis des vereinbarten Retainer-Modells. Durch die Kombination aus Retainer und flexiblem Abruf wird sichergestellt, dass kurzfristige Reaktionsfähigkeit und planbare Kostenstrukturen gewährleistet sind. Der AN dokumentiert alle Tätigkeiten im Rahmen der erbrachten Dienstleistung inklusive der erbrachten Stunden und stellt diese der TK zur Verfügung.

### **4 Abruf der Dienstleistung**

Berechtigungen bei der TK für den Abruf der Dienstleistung werden im gemeinsamen initialen Workshop (Kickoff-Termin) zwischen der TK und dem AN festgelegt.

Um eine gesicherte Kommunikation von vermuteten oder bereits erfolgreichen Angriffen bzw. einer Kompromittierung von IT-Systemen zu nutzen, MUSS der AN eine elektronische verschlüsselte Schnittstelle (z.B. Ticketsystem) für die Meldung und Datenübertragung zur Verfügung stellen.

Der AN MUSS sich bei der Wahl von TLS-Version(en) und der eingesetzten Cipher-Suites an die Empfehlungen der jeweils aktuellen Fassung der Technischen Richtlinie BSI *TR-02102-2 "Kryptographische Verfahren: Verwendung von Transport Layer Security (TLS)"* des BSI halten. Dabei stellt der AN sicher, dass alle Kommunikationsteilnehmer mindestens eine der zulässigen Cipher-Suites unterstützen. Der AN gleicht die von ihm gewählte Konfiguration mindestens jährlich gegen die Vorgaben des BSI ab. Bei Abweichungen passt der AN die Konfiguration an, um Konformität mit der o.a. Richtlinie herzustellen.

Für den telefonischen Kontakt zur Meldung eines vermuteten oder bereits erfolgreichen Angriffs bzw. einer Kompromittierung von IT-Systemen MUSS der AN eine dauerhaft verfügbare (24 Stunden am Tag, 7 Tage die Woche, 365 Tage im Jahr) Notfallnummer anbieten, um eine schnelle Reaktion zu ermöglichen.

## **5 Qualifizierung**

### **5.1 Fachexpertise IT-Forensiker:in**

Der AN MUSS für die Dienstleistung des Incident Response und Forensik Services qualifizierte Mitarbeitende stellen. Diese besitzen mindestens folgende Qualifizierungen:

- 5 Jahre Berufserfahrung im Bereich Incident Response und Forensik
- Gute Deutschkenntnisse (C1) in Schrift und Sprache

Die Mitarbeitenden SOLLEN mindestens eine der folgenden Zertifizierungen haben:

- GIAC Certified Forensic Analyst
- GIAC Certified Incident Handler

Der/Die Verhandlungsführer:in SOLL eine Zertifizierung als Vorfall-Experte besitzen. Beim AN SOLLEN mindestens 10 Forensiker:innen mit dem Aufgabenschwerpunkt IT-Forensik beschäftigt werden.

### **5.2 Zertifizierung, Testate und Nachweise**

Der AN MUSS zum Zeitpunkt der Leistungserbringung nach ISO/IEC 27001 zertifiziert sein.

Der AN MUSS als qualifizierter Advanced Persistent Threat Response-Dienstleister beim BSI gelistet sein.

Sofern der AN im Rahmen des eingesetzten Cloud-Computing-Dienstes Sozialdaten verarbeitet, erbringt er die Leistungen unter Einhaltung der Anforderungen des § 393 SGB V und der zugehörigen C5-Gleichwertigkeitsverordnung. Ein aktuell gültiges C5-Testat MUSS dann mindestens jährlich gegenüber der TK nachzuweisen bei einem Einsatz von Cloud-Computing bei der Verarbeitung von Sozialdaten. Bei unterjährigen - für die TK relevanten - Änderungen des Testats ist die TK unverzüglich zu informieren.

## **6 Organisatorische und technische Anforderungen in der Informationssicherheit**

Die Vorgaben zu organisatorischen und technischen Anforderungen in der Informationssicherheit sind der Anlage L1 „Vertragsanlage\_Informationssicherheit“ zu entnehmen.

## **7 Datenschutz**

Auf den Systemen der TK werden sensible Sozial- und Gesundheitsdaten verarbeitet. Im Rahmen der Auswertung und Untersuchung von IT-Systemen kann daher nicht ausgeschlossen werden, dass der AN Einsicht in derartige Daten erhält. Hierzu ist es zwingend erforderlich, dass Daten, welche Sozial- oder Gesundheitsinformationen enthalten, nur innerhalb des europäischen Wirtschaftsraums, in der Schweiz oder in Großbritannien. Auch die Einsichtnahme darf nur aus den Wirtschaftsräumen oder genannten Ländern erfolgen.

Der AN hat in diesem Zusammenhang die Anforderungen zur Verarbeitung von Daten im Auftrag gem. Art. 28 DSGVO in Verbindung mit § 80 SGB X zu erfüllen (siehe Anlage XXX).

Daten, welche explizit im Einzelfall durch die TK von dieser Regelung ausgenommen werden (z.B. Malware-Samples), können auch in einer anderen Jurisdiktion verarbeitet werden.