Bundesamt
für Sicherheit in der
Informationstechnik



**Kriterien für qualifizierte Dienstleister**

# APT-Response-Dienstleister

Aufgrund zunehmender, massiver Cyber-Angriffe auf Unternehmen und staatliche Institutionen besteht neben der Prävention auch ein steigender Bedarf zur Abwehr laufender oder erfolgter Angriffe. Besonders bei gezielten Angriffen starker Gegner (Advanced Persistent Threat, APT) stellen diese Tätigkeiten spezielle Anforderungen an die dabei eingesetzten Dienstleister.

Merkmale solcher gezielten Angriffe / APTs sind:

- Gezielter Angriff auf ausgewählte Organisationen
- Typischerweise Einsatz verschiedener Angriffstechniken
- Persistente (d.h. dauerhafte) Bedrohung / Infektion
- Starker, d.h. mit umfangreichen Ressourcen und Know-How versehener Angreifer
- Ausbreitung im internen Netz

## 1 Definition APT-Response-Dienstleister

### 1.1 Aufgaben eines APT-Response-Dienstleisters

Zu den charakteristischen Aufgaben eines APT-Response-Dienstleisters gehören:

- Aufklärung des Umfangs des Angriffs und der aktiven Zugangskanäle
- Aussperrung des Angreifers
- Beobachtung neuer Angriffsversuche und Ursachenanalyse
- Säuberung manipulierter Systeme und Verhinderung erneuter Vorfälle
- Optional: Suche und Erkennung möglicher Angriffe (APT-Hunting)

### 1.2 Typischer Projektablauf

Der Projektablauf bei Response-Projekten ist sehr individuell und von der Art des Angriffs abhängig, beinhaltet aber typische Kernelemente:

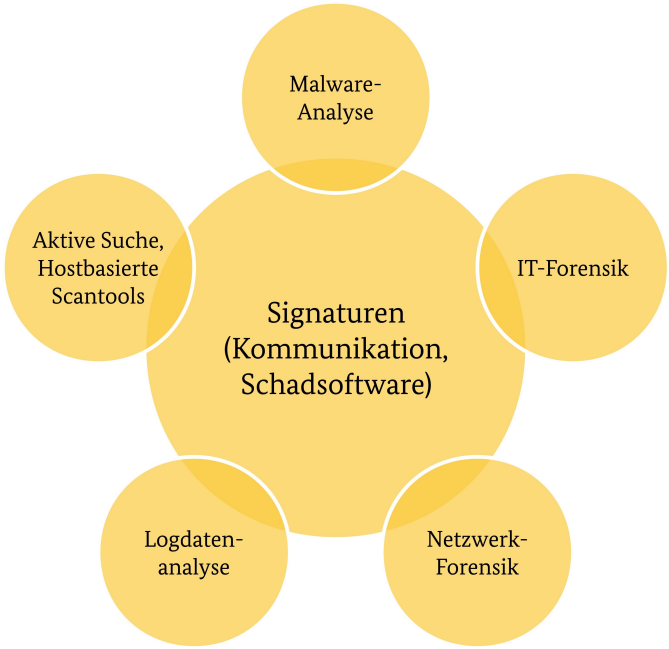
**Vorfeld**
Ein Response-Projekt beginnt in aller Regel durch ein auslösendes Ereignis. Dabei kann es sich um die Erkennung eines Angriffs handeln oder (häufiger) um das Auftreten von Indizien, die einen erfolgten oder laufenden Angriff vermuten lassen. Dabei ist der Dienstleister üblicherweise noch nicht involviert, auch wenn eine Beratungstätigkeit zu Erkennungsmöglichkeiten außerhalb eines konkreten Response-Projekts zum Kompetenzbereich des Anbieters zählen sollte.

**Erstbegutachtung**
Als erste Reaktion auf einen Vorfallsverdacht wird der Dienstleister eine Erstbegutachtung und -analyse der betroffenen Systeme durchführen. Hier entscheidet sich die weitere Vorgehensweise.

- Etablierung sicherer Kommunikationskanäle unter Umgehung möglicherweise betroffener Systeme
- Welche Spuren wurden bereits aufgenommen? Welche Maßnahmen wurden bereits getroffen?
- Gibt es eine Malware-Beteiligung?
- Ist der Angreifer[1] noch aktiv? Könnte er Reaktionen beobachten?
- Wie sieht die betroffene Infrastruktur im Überblick aus? Wie gut kennt die betroffene Organisation ihre Infrastruktur?
- Über welche Zugriffswege verfügt der Angreifer wahrscheinlich?
- Welche Monitoring- und Beobachtungsmöglichkeiten sind vorhanden? Welche werden benötigt?
- Ist (wahrscheinlich) eine gerichtsfeste Dokumentation notwendig?[2]

### Analyse

Im Rahmen der Vorfallsbehandlung werden weitere Analysen und Beobachtungen durchgeführt. Ziel ist mittelfristig das dauerhafte Aussperren des Angreifers (dazu bedarf es aber einer fundierten Analyse des Ausmaßes der Kompromittierung); anschließend die Unterstützung bei der Bereinigung und die Feststellung entstandener Schäden.




Die Analysen können aus verschiedenen Untersuchungen bestehen:

- IT-Forensische Untersuchungen von betroffenen Client- und Serversystemen,
- Auswertung von Protokolldaten (z. B. Web-Proxy, Firewall-Logs, Betriebssystem- und Anwendungslogs, ...),
- Netzwerkforensik,
- Malware-Analyse (dynamische und statische Analyse evtl. eingesetzter Schadsoftware),
- Recherche zum tatsächlichen Aufbau der Infrastruktur und zur Konfiguration von Firewalls und ähnlichen Systemen zum Zeitpunkt des Angriffs

Die Ergebnisse jeder Analysephase sind dabei – neben direkten Erkenntnissen über den Angreifer und den Schaden – weitere Anhaltspunkte und „Signaturen“ („Indicators of Compromise“), anhand derer weitere Ermittlungen durchgeführt werden können.

Dafür werden bestehende Protokollierungs- und Beobachtungssysteme des Auftraggebers genutzt oder neue Beobachtungsmöglichkeiten speziell geschaffen.

Wenn der Angreifer noch aktiv ist, sollte er die Beobachtung nicht bemerken, um Gegenmaßnahmen (Vertuschung und Löschen von Spuren, aktive Gegenangriffe) zu vermeiden. Daher sollten aktive Maßnahmen wie Netzwerksperrungen, Bereinigungen von Systemen, Passwortwechsel etc. erst dann durchgeführt werden, wenn die Analyse abgeschlossen ist und die Bereinigung als Gesamtschritt möglich ist. Dies unterstützt das Ziel die Angriffskampagne zu erkennen und verhindert mögliche Schäden durch zerstörerische Aktionen des Angreifers.

Die Analysephase läuft daher anfangs exklusiv und nicht parallel zur Aussperrung und Bereinigung .

1 Bei APT-Angriffen ist i. d. R. von mehreren, gut organisierten Täterinnen und Tätern auszugehen. Aus Gründen der sprachlichen Vereinfachung wird im weiteren vereinfachend von „dem Angreifer“ gesprochen.

2 Eine gerichtsfeste Dokumentation verursacht in der Regel einen höheren Aufwand; da allerdings die Entscheidung gegen eine gerichtsfeste Dokumentation nicht mehr nachträglich korrigierbar ist, muss ein Minimum an Dokumentation bei der Erfassung und Analyse immer vorhanden sein.

**Aussperren**
Der Angreifer kann nur ausgesperrt werden, sobald möglichst genau geklärt ist, über welche Zugriffswege er verfügt, und ob ein erneutes Eindringen erkannt und nachvollzogen werden kann.

Neben der Unterstützung bei der technischen Umsetzung berät der Dienstleister den Auftraggeber auch über mögliche betriebliche Risiken der Maßnahmen und sorgt für eine koordinierte Umsetzung.

**Bereinigung**
Auch nach der Aussperrung werden die Analysen und Beobachtungen fortgeführt, um das Ausmaß des Schadens besser bestimmen, und um ein erneutes Eindringen identifizieren zu können.

Auf der Basis der Analyseergebnisse unterstützt der Dienstleister den Auftraggeber bei der Erstellung eines Plans zur Wiederherstellung des Normalbetriebs und bei der vollständigen Säuberung der Systeme.

Die Art der Säuberung hängt dabei von den spezifischen Untersuchungsergebnissen ab. Üblicherweise werden Systeme, die unter direkter Kontrolle des Angreifers standen, neu aufgesetzt.

Der Dienstleister unterstützt den Auftraggeber bei der Abwägung und Risikobeurteilung, auf Wunsch auch bei der Umsetzung der Säuberungsmaßnahmen.

**Weitere Untersuchungen und Beratung**
In Absprache mit dem Auftraggeber können nach der Bereinigung noch weitere Fragestellungen untersucht werden. Dazu gehören unter anderem:

- Bestimmung des Schadenausmaßes: Von welchen Informationen hat der Angreifer Kenntnis erhalten? Lassen sich Systeme und Daten abgrenzen, die vom Angriff nicht betroffen waren?
- Welche Empfehlungen zum weiteren Vorgehen lassen sich aus den Untersuchungserkenntnissen ableiten?

Neben den konkreten Lücken und Hintertüren, die in der Bereinigung unschädlich gemacht werden, decken die Untersuchungen häufig auch strukturelle Mängel in der Sicherheitsarchitektur auf.

### 1.3 Aufgabenbereiche bei einem Response-Projekt

Ein Response-Projekt deckt damit verschiedene Aufgabenbereiche ab, die jeweils eigene Qualifikationen benötigen.

**Ermittlungsleitung**
Bei einem APT-Vorfall ist meist eine größere Zahl von Systemen innerhalb einer Institution sowie bei deren Partnern (Outsourcingprovidern, Dienstleistern, verbundenen Unternehmen) betroffen. In einem Response-Projekt müssen daher das Vorgehen und die Unterstützung mit vielen internen und externen Ansprechpartnern abgestimmt werden. International wird diese Tätigkeit im Rahmen der „Incident Response" auch als „Incident Manager" („ENISA Good Practice Guide for Incident Management") oder „Incident Lead" (NIST SP 800-61) bezeichnet.

Dabei sollte die Ermittlungsleitung insbesondere auch die entsprechenden Datenschutzbestimmungen, denen die beauftragende Institution unterliegt, berücksichtigen und dafür Sorge tragen, dass sowohl alle Ansprechpartner als auch die eigenen Mitarbeiter über die Bestimmungen informiert werden. Des Weiteren sollte der Datenschutzbeauftragte sowie der Personal- bzw. Betriebsrat der beauftragenden Institution frühestmöglich über die geplanten Arbeiten informiert und in weitere Schritte eingebunden werden.

Die Ermittlungsleitung koordiniert daher zum einen die Arbeit der Mitarbeiter im Ermitt-

lungsteam:[3]

- Kurzfristige Personaldisposition bei Einsatzbeginn und als Reaktion auf neue Erkenntnisse
- Beschaffung der nötigen Infrastruktur vor Ort
- Projektmanagement mit besonderem Fokus auf einen ständigen Informationsaustausch

Darüber hinaus unterstützt die Ermittlungsleitung den Auftraggeber bei der Einschätzung und Koordination von weiteren Arbeiten:

- Regelmäßige Statusupdates ggf. in verschiedenen Detaillierungsgraden
- Regelmäßige Übersicht über noch vom Auftraggeber zu beschaffende Informationen, Systeme und Installationen
- Direkte Abstimmung mit Dienstleistern und Mitarbeitern des Auftraggebers in dessen Auftrag
- Sicherstellung der vereinbarten Vertraulichkeit
- Risikomanagement über die projektspezifischen Risiken

In der Regel unterstützt der Ermittlungsleiter auch das Krisenmanagement. Die spezifischen Tätigkeiten im Krisenmanagement sind im Abschnitt „Unterstützung beim Krisenmanagement“ beschrieben.

### Malware-Analyse

Wird auf einem der Systeme verdächtige Software (Malware) gefunden, muss diese in einer gesicherten Umgebung analysiert werden. Die Analyse verfolgt mehrere Ziele:

- Bestimmung der Fähigkeiten der Malware, um das Ausmaß des Angriffs abschätzen zu können und Komponenten und Systeme für die Bereinigung zu bestimmen
- Ableiten von Indikatoren für einen Befall (Indicators of Compromise, IOC), damit weitere Systeme systematisch auf die Malware untersucht werden können
- Sammeln von Indizien für die Herkunft der Malware und damit möglicherweise des Angriffs

Da in einem APT-Vorfall üblicherweise speziell für den Angriff zusammengestellte Malware zum Einsatz kommt, ist eine automatisierte Prüfung mit externen Malwareerkennungssystemen nicht ausreichend. Zudem verbieten Anforderungen an die Vertraulichkeit häufig die Übermittlung von verdächtigen Dateien an Dritte; auch weil dadurch eine frühzeitige Warnung des Angreifers nicht ausgeschlossen werden kann.

Bei der Analyse werden in der Regel die folgenden Techniken eingesetzt:

- Ausführen in einer gesicherten Umgebung (Sandbox, dynamische Analyse)
- Analyse des Programmcodes durch Reverse Engineering (Disassemblieren, statische Analyse)
- Techniken, um Schutzmaßnahmen der Malware gegen diese Analysen zu umgehen

### Host-Forensik

Systeme, die im Verdacht stehen, vom Angriff betroffen zu sein, werden mit den Mitteln der Host-Forensik untersucht. Im ersten Schritt müssen die zu analysierenden Daten erhoben werden. Die Datenakquise geschieht durch

- IT-forensische Abbilder des Hauptspeichers
- das nachvollziehbare Sicherstellen von Datenträgern und vollständigen Systemen
- IT-forensische Abbilder von Festplatten und anderen Speichermedien
- Sicherstellen von Protokolldaten und Datensicherungen

Die konkrete Art der Datenakquise wird im Einzelfall unter Berücksichtigung der forensischen Fragestellung und der betrieblichen Anforderungen des Auftraggebers gewählt.

Bei der Aufklärung von APT-Vorfällen ist eine gerichtliche Aufarbeitung des Angriffs meist nachrangig. Für eine gerichtsfeste Sicherstellung müssen aber direkt bei der Datenakquise

3 Das Ermittlungsteam kann gerade bei größeren Fällen auch Forensiker des betroffenen Unternehmens bzw. Mitarbeiter anderer Dienstleister des betroffenen Unternehmens umfassen, die mit koordiniert werden müssen.

Maßnahmen getroffen werden, insbesondere muss eine erweiterte Dokumentation geführt werden. Der IT-Dienstleister muss eine gerichtsfeste Dokumentation sicherstellen können.

Forensische Fragestellungen der Analyse können unter anderem sein:

- Identifikation des initialen Infektionsweges
- Hinweise auf weitere betroffene Systeme und Nutzerkonten
- Muster bei der Vorgehensweise des Angreifers, die als Indikatoren für einen Befall (IOC) dienen können, um die Systeme systematisch auf Angriffsspuren untersuchen zu können
- Erkennbarer Datenabfluss
- Nachweise und Indizien für die Herkunft des Angriffs

Da bei einem APT-Vorfall Systeme unterschiedlicher Hersteller mit verschiedenen Softwareinstallationen betroffen sein können, sollte der IT-Dienstleister neben der Windows-Plattform über plattformübergreifende Analysefähigkeiten verfügen.

### Netzwerkforensik

Der Angriff kann auch durch Beobachtung des Netzwerkverkehrs nachvollzogen werden. Auch die Wirksamkeit der Gegenmaßnahmen kann auf dieses Weise überwacht werden. Als Ausgangspunkt für die Netzwerkforensik dienen

- Bereits installierte Beobachtungs- und Protokollierungssysteme
- Gesicherte Netzwerkprotokolldaten, soweit vorhanden
- Speziell für die Vorfallsbehandlung in das Netzwerk eingebrachte Beobachtungssysteme
- Bereits installierte oder neu aufgebaute Systeme, um die Beobachtungen zu sammeln und korreliert bewerten zu können

Zu den Aufgaben der Netzwerkforensik gehören auch die Erhebung möglicher Datenquellen und die Identifizierung von zusätzlichen Beobachtungsmöglichkeiten zusammen mit dem Auftraggeber und dessen Dienstleistern. Die Mitarbeiter im Bereich Netzwerkforensik unterstützen den Auftraggeber bei der Umkonfiguration von bestehenden Systemen und beim Aufbau von neuen Systemen.

Mit Hilfe der so erhobenen Daten können ähnliche forensische Fragestellungen wie bei der Host-Forensik beantwortet werden:

- Identifikation des initialen Infektionsweges (falls Daten aus dieser Zeit vorliegen)
- Aktuelle Vorgehensweise des Angreifers
- Hinweise auf weitere betroffene Systeme und Nutzerkonten
- Muster bei der Vorgehensweise des Angreifers, die als Indikatoren für einen Befall (IOC) dienen können, um die Systeme systematisch auf Angriffsspuren untersucht zu können
- Erkennbarer Datenabfluss
- Nachweise und Indizien für die Herkunft des Angriffs
- Spuren von neuerlichen Aktivitäten des Angreifers nach den ersten Gegenmaßnahmen und dem abschließenden Ausschluss

### Sicherheitsfokussierte Unterstützung im IT-Bereich

Der Dienstleister unterstützt den IT-Betrieb des Auftraggebers dabei, Beobachtungsmöglichkeiten auszubauen, die ersten Gegenmaßnahmen einzuleiten und den Angreifer auszusperren.

- Erkenntnisse aus der Erstbegutachtung und der verschiedenen forensischen Analysen werden dafür speziell aufbereitet
- Der Vorfall und dessen Folgen werden unter Berücksichtigung der getroffenen Regeln zur Vertraulichkeit auch innerhalb des Unternehmens mit den IT-Mitarbeitern und Dienstleistern besprochen.
- Empfehlungen und Bewertungen für Erstmaßnahmen werden abgegeben
- Der Auftraggeber wird bei der koordinierten Aussperrung des Angreifers unterstützt.

- Teilweise werden auch der Aufbau und der Betrieb von Systemen während der Vorfallsbehandlung übernommen.
- Basierend auf den identifizierten Indicators of Compromise werden Werkzeuge zur Verfügung gestellt, um alle Systeme des Auftraggebers systematisch auf Spuren des Angriffs prüfen zu können.

**Bereinigung betroffener Systeme**

Nach erfolgter Sicherung und Analyse der betroffenen Systeme müssen diese Systeme in einen bereinigten Zustand überführt werden. Der IT-Dienstleister unterstützt den Auftraggeber bei der Durchführung der notwendigen Tätigkeiten, z. B.:

- Neuaufsetzung der Systeme
- Einspielung von Backups
- Wechsel von Passwörtern

**Unterstützung beim Krisenmanagement**

Der Angriff, aber auch die Auswirkungen der Erstmaßnahmen, können den Geschäftsbetrieb massiv stören. Der IT-Dienstleister unterstützt den Auftraggeber auch durch

- Beratung zu notwendigen Entscheidungen und Prozessen
- Bewertung des Risikos für weitere Schäden
- Unterstützung bei der Kommunikation innerhalb des Unternehmens und mit Externen (beispielsweise Presse und Kunden)
- Unterstützung bei der Umsetzung eines Notbetriebs und geordneter Übergang wieder zurück zum Normalbetrieb
- Unterstützung bei der Einberufung und Organisation eines Krisenstabs

## 1.4 Rollen

Die Themenbereiche bei dem Response-Projekt bilden sich direkt auf mögliche Rollen ab. Die Grenzen werden anhand der vorherigen Aufgabenbeschreibungen gezogen, sodass sich aus den erforderlichen Wissensgebieten und Erfahrungen abgeschlossene Rollenprofile ergeben. Dabei sind üblicherweise mehrere der Themenbereiche in einer Person vereint:

- Ermittlungsleiter (organisatorisch -technisch)
- IT-Sicherheitsspezialist (technisch -organisatorisch)
- Krisenmanager (organisatorisch)
- Malware-Analyst (technisch)
- Host-Forensiker (technisch)
- Netzwerkforensiker (technisch)

Je nach Art des Vorfalls werden nicht alle Rollen benötigt. Der Bedarf entwickelt sich jedoch oftmals erst während der fortschreitenden Analyse des Angriffs. Dabei können einzelne Personen auch mehrere – im Extremfall alle – Rollenprofile abdecken.

Die Rollen bilden die Grundlage für die Kompetenzanforderungen, wie sie in 2 beschrieben werden.

## 1.5 Optional: APT-Hunting

Besteht bisher lediglich der Verdacht auf einen Angriff, oder soll präventiv nach Indizien für eine Kompromittierung gesucht werden, kann APT-Hunting zum Einsatz kommen, um so Klarheit über einen ggf. erfolgten gezielten Angriff zu erlangen. Dabei sollte der Dienstleister in der Lage sein große Datenmengen zu analysieren, ohne sich in diesem Fall ausschließlich auf automatisierte Techniken und Signaturen zu verlassen. Eine schnelle Einschätzung stellt hierbei das Ziel dar, um bei einem tatsächlich stattfindenden Angriff die geeigneten Gegenmaßnahmen einzuleiten, wie sie in 1.2 dargestellt werden.

# 2 Kriterien

APT-Response-Dienstleister müssen die folgenden personellen, organisatorischen und technischen Voraussetzungen erfüllen:

## 2.1 Personelle Voraussetzungen des Teams

Der Dienstleister definiert ein „Kernteam“ von Personen, welches bei einem APT-Vorfall schnell einsatzbereit sein muss. Die Personen im Kernteam des Dienstleisters müssen als Team alle in den folgenden Unterabschnitten geforderten Eigenschaften und Fachkenntnisse mitbringen.

### Grundlegende persönliche Eigenschaften

Die folgenden persönlichen Eigenschaften sind Grundlage aller Rollen:

- Teamfähigkeit
- Unbeeinflussbarkeit und Unvoreingenommenheit
- Fähigkeit, Vertraulichkeit der im Projekt gewonnenen Erkenntnisse gegenüber Dritten zu wahren
- Unbestechlichkeit
- Integrität
- Zielorientiertes Denken und Handeln
- Ausgeprägte analytische Fähigkeiten
- Fähigkeit zur sachlichen Ergebnisdarstellung (Trennung von Fakten und Vermutungen)
- Bereitschaft zur Weiterbildung
- Belastbarkeit
- Beherrschung der deutschen und gute Kenntnisse der englischen Sprache

### Ermittlungsleiter

Der Ermittlungsleiter muss zusätzliche persönliche Eigenschaften mit sich bringen:

- Fähigkeit zur Team-Leitung
- Fähigkeit zur Koordination verschiedener Dienstleister
- Fähigkeit zur laufenden, sachlichen und zielgruppenorientierten Kommunikation
- Erstellen von Lagebildern
- Zielgruppengerechte Darstellung technischer Fakten, auch gegenüber technischen Laien
- Bewertung des Sachverhalts
- Darlegung notwendiger Maßnahmen
- Managen von Konflikten
- Überzeugungsfähigkeit

Für die Ausübung der Rolle sind folgende Kenntnisse und Erfahrungen notwendig:

- Praktische Berufserfahrung in der Vorbereitung und Durchführung von Response-Projekten in einer (mit)verantwortlichen Rolle sowie Berufserfahrung in mindestens einer der technischen Rollen
- Personaldisposition
- Risikomanagement über die projektspezifischen Risiken
- Datenschutzbestimmungen

### IT-Sicherheitsspezialist

Der IT-Sicherheitsspezialist muss zusätzlich umfassende Kenntnisse aus dem Bereich der IT- und Informationssicherheit in den folgenden Bereichen aus praktischer Berufserfahrung mit sich bringen, vor allem auch:

- Kenntnisse im Bereich der Systemadministration: Oft müssen kurzfristig Maßnahmen im Netz

des Betroffenen umgesetzt werden, z. B. um den Angreifer auszuschließen, um hinterlassene Hintertüren zu schließen, zusätzliche Beobachtungsmöglichkeiten zu schaffen, oder mehr Informationen einzusammeln. Oft fehlt dazu Know-how beim Kunden, sodass er unterstützt werden muss. Dazu ist es unerlässlich, Vorgehen, Prozesse und Werkzeuge im Bereich der Systemadministration zu kennen.

- Betriebssystemspezifische Kenntnisse im Bereich Windows (insbesondere Domänenstrukturen und Gruppenrichtlinien) und Linux (im Serverbereich)
- Kenntnisse im Bereich des Sicherheitsmanagements: Standardansätze zum Informationssicherheitsmanagement (u.a. ISO 27001 ff., BSI-Grundschutz) müssen bekannt sein.
- Kenntnisse im Bereich von IT-Sicherheitsprodukten: Der IT-Sicherheitsspezialist muss in der Lage sein, Beratung zur gezielten Konfiguration und Einsatz bestehender bzw. neuer IT-Sicherheitsprodukte, z.B. Intrusion Detection, Firewall, Anti Virus, im Rahmen des Response-Projekts zu geben.

### Krisenmanager

Der Krisenmanager muss zusätzliche persönliche Eigenschaften mit sich bringen:

- Beherrschung von Moderationstechniken
- Gute organisatorische Fähigkeiten
- Fähigkeit zur Behandlung von Einwänden
- Fähigkeit zum Managen von Konflikten
- Überzeugungsfähigkeit

Der Krisenmanager benötigt

- Kenntnisse und praktische Erfahrung im Bereich des Krisenmanagements.
- Kenntnisse im Öffentlichkeitsmanagement

### Malware-Analyst

Der Malware-Analyst muss zusätzlich vor allem über die folgenden praktischen Kenntnisse im Bereich der Malware-Analyse verfügen:

- Statische Analyse: Analyse von Binary-Formaten; Code-Analyse; Umgang mit „Binary Packern“, AV-Scannern, Disassemblern und gängigen Software-Tools zur statischen Analyse
- Dynamische Analyse: Untersuchung verdächtiger Software in kontrollierter Umgebung unter einem Debugger, Instrumentieren einer Sandbox-Umgebung, Umgang mit üblichen Software-Tools zur dynamischen Analyse.
- Speicherforensik: Aufnahme und Analyse von Speicherabbildern
- Betriebssysteminterna: Gute Kenntnisse von Betriebssysteminterna gängiger Betriebssysteme bilden die Grundlage für die Beurteilung der Funktion und Auswirkungen von Schadsoftware. Von Malware genutzte API-Funktionen geben meist erste Hinweise auf den Charakter einer Software.
- Programmiersprachen: Kenntnis gängiger Programmier- und Skriptsprachen, auch Assemblersprachen, ist Grundlage für die Beurteilung der Funktion der Malware.

### Host-Forensiker

Der Host-Forensiker benötigt zusätzlich genaue Kenntnisse seiner Werkzeuge und ausreichende Praxis:

- Forensische Beweissicherung: Erfahrung in den Grundlagen forensischer Beweissicherung, Dokumentation und Nachweis (z. B. durch kryptographische Prüfsummen).
- Forensische Datensicherung: Erfahrung im Erstellen forensischer Abbilder von Speichermedien (vor allem Festplatten und SSDs) in verschiedenen Umgebungen. Dies umfasst insbesondere Kenntnisse der „Live“-Sicherung, Sicherung in verschiedenen Virtualisierungsumgebungen, Sicherung bei laufenden Systemen.
- „Live-Akquise“: Vitale Daten können nur zur Laufzeit erhoben werden. Daher ist die Erstellung von Hauptspeicherabbildern, die Aufnahme von Prozess- und Netzwerkinformationen, erforderlich.
- Forensische Analyse: Es müssen sichere Kenntnisse über übliche Dateisysteme und Betriebssysteme vorhanden sein. Notwendig ist der sichere Umgang mit ein oder mehreren integrierten forensischen Untersuchungsumgebungen sowie forensischen Tools für die Auswertung häufiger Spuren (z. B. Windows-Registry, Browserhistorie, Mail, Systemlogs usw.). Kenntnisse in der Analyse

von Protokolldaten und zugehöriger Softwaretools werden ebenfalls benötigt.

- Betriebssysteminterna: Gute Kenntnisse von Betriebssysteminterna gängiger Desktop-, Server- und mobiler Betriebssysteme bilden die Grundlage für die Analyse forensischer Artefakte auf den untersuchten Systemen. Der Umgang mit üblichen Log- und Monitoring-Formaten (Windows Eventlog, Syslog) ist notwendig. Kenntnisse häufig genutzter Anwendungen sollten ebenfalls vorhanden sein.
- Lateral-Movement: Erfahrungen mit der Analyse von Lateral-Movement. Unter Lateral-Movement versteht man Techniken, mit dem es einem Angreifer ermöglicht wird Zugriff und Kontrolle über Remote-Systeme im Netzwerk zu erlangen. Mit der Hilfe der Techniken wird dabei ein Angreifer in die Lage versetzt, Informationen von Systemen zu erhalten, ohne zusätzliche Remote-Access-Tools einsetzen zu müssen.

#### Netzwerkforensiker

Der Netzwerkforensiker muss zusätzlich vor allem folgende praktische Kenntnisse mit sich bringen:

- Gute Kenntnisse im Bereich Netzwerkprotokolle (TCP/IP), Umgang mit Protokolldekodern und Auswertungssoftware für große Datenmengen
- Kenntnisse im Bereich von Netzwerkgeräten (Router, Switches) sowie IT-Sicherheitsprodukten im Netzbereich (z. B. Firewalls, IDS, usw.)
- Programmiersprachen: Kenntnis gängiger Programmier- und Skriptsprachen
- Firewall-Analyse: Auswertung der Log-Daten der Firewall
- Lateral-Movement (siehe Host-Forensiker)

#### Weitere unterstützende Rollen

Im Rahmen eines Response-Projektes werden weitere Rollen benötigt, die durch den IT-Dienstleister besetzt, besser jedoch durch die betroffenen Stellen selbst abgedeckt werden sollten:

- Zugriff auf IT-Sicherheit und auf Einsatzunterstützung spezialisierte Juristen
- Zugriff auf Kommunikationsberatungsunternehmen für die Krisenkommunikation mit der Öffentlichkeit und Kunden / Partnern

### 2.2 Organisatorische Voraussetzungen

Der Dienstleister muss zur Vorbereitung zukünftiger Einsätze bereits vorbereitende Maßnahmen treffen, um die zeitaufwändigen Arbeiten in der Einsatzphase bestmöglich zu unterstützen. Dazu gehören:

- Vorlagen für Berichte und Dokumentationen
- Muster bzw. teilvorausgefüllte Auftragsdatenverarbeitungserklärungen
- Auflistung der betroffenen Systeme sowie Artefaktsammlung
- Mustervorgehensweise zur Managementberatung
- Grundlagenvortrag  zum Thema APT für das Management, den Personalrat und Hinweise zum Datenschutz mit allgemeinen Punkten sowie Maßnahmen zum Vorgehen.
- Vorbereitung für die Zusammenarbeit mit Dritten Teams
- Geeignete Quellen für Indicators of Compromise (IOC) müssen verfügbar sein

Des Weiteren muss sichergestellt sein, dass sowohl die Ausrüstung als auch die Personen des „Kernteams“ schnell zum Einsatzort gelangen könnten. Entsprechende Transportmöglichkeiten sollten Vorgehalten werden oder kurzfristig zur Verfügung stehen.

### 2.3 Technische Voraussetzung für Host-Forensik, Netzwerkforensik und Malware-Analyse

#### IT-Forensisches Labor

Der IT-Dienstleister muss über die notwendigen technischen Voraussetzungen zur Durchführung von forensischen Untersuchungen verfügen. Dazu gehört ein separates IT-forensisches Labor mit der Möglichkeit zur manipulationsgeschützen Akquise von Daten und zur nachvoll-

ziehbaren forensischen Analyse der Daten: Mindestens für folgende Aktivitäten müssen entsprechende Hard- bzw. Software im Labor bereitstehen und die Mitarbeiter für den fachkundigen Einsatz ausreichend geschult sein:

- Schreibgeschütztes Kopieren von Datenträgern (Festplatten, Solid State Disks)
- Erstellen von Abbildern des Hauptspeichers unter gängigen Betriebssystemen
- Erstellung und Prüfen von kryptographischen Hashwerten für einzelne Dateien und Abbilder von Festplatten
- Wiederherstellen von gelöschten Daten in gängigen Dateisystemen
- Extraktion von Metadaten aus gängigen Dateisystemen, gelöschten Fragmenten und Dateien
- Analyse von Protokolldaten (textuelle Formate und Binärformate)
- Indizierung und effiziente Suche in den sichergestellten Daten
- Entschlüsselung von Festplatten und Dateien soweit die nötigen Schlüssel vom Auftraggeber zur Verfügung gestellt werden
- Rekonstruktion von verschleierten Daten zum Beispiel durch Brechen von einfachen Verschlüsselungen mit leicht erratbaren Passwörtern (Wörterbuchangriffe)
- Protokollierung der durchgeführten Analyseschritte

Die Ausstattung muss die Analyse verschiedener Systeme ermöglichen, dabei sollten die aktuell gebräuchlichsten Hard- und Software-Kombinationen abgedeckt werden.

### Labor zur Malware-Analyse

Der IT-Dienstleister muss über die notwendigen technischen Voraussetzungen zur Analyse von Malware verfügen. Dazu gehört ein Labor mit der Möglichkeit, Malware in einer geschützten Umgebung auszuführen (dynamische Analyse) sowie durch Reverse Engineering (Disassemblierung, statische Analyse) analysieren zu können. Mindestens für folgende Aktivitäten müssen entsprechende Hard- bzw. Software bereitstehen und die Mitarbeiter für den fachkundigen Einsatz ausreichend geschult sein:

- Geschützte Umgebung zum Ausführen und Beobachten von Malware unter verschiedenen Betriebssystemen
- Schrittweises Ausführen und Manipulieren der Ausführung der Malware (Debugging)
- Umgehung von Abwehrtechniken der Malware gegen die Analyse (Antidebugging-Techniken, Virtualisierungserkennung)
- Disassemblierung der Malware und statische Analyse
- Rekonstruktion von sich selbst entpackenden und modifizierenden Programmen
- Ableitung von Indikatoren für einen Befall (IOC)
- Rekonstruktion von verschleierten Daten zum Beispiel durch Brechen von einfachen Verschlüsselungen mit leicht erratbaren Passwörtern durch systematisches Ausprobieren (Wörterbuchangriffe)
- Protokollierung der durchgeführten Analyseschritte

Die Ausstattung muss die Analyse verschiedener Systeme ermöglichen, dabei sollten die aktuell gebräuchlichsten Betriebssysteme abgedeckt werden.

### Mobil einsetzbare Ausstattung

Der IT-Dienstleister muss über die notwendigen technischen Voraussetzungen zur Durchführung von forensischen Untersuchungen bei dem Auftraggeber vor Ort verfügen. Dazu gehört mindestens eine ausreichende mobile Ausstattung, um die Datenakquise vor Ort durchführen zu können.

Mindestens für folgende Aktivitäten muss entsprechende Hard- bzw. Software bereitstehen, die kurzfristig beim Auftraggeber eingesetzt werden kann, und die Mitarbeiter für den fachkundigen Einsatz ausreichend geschult sein:

- Schreibgeschütztes Kopieren von Datenträgern

- Erstellen von Abbildern des Hauptspeichers
- Erstellung und Prüfen von kryptographischen Hashwerten für einzelne Dateien und Abbilder von Festplatten
- Analyse des laufenden Systems unabhängig von der darauf installierten, möglicherweise manipulierten Software
- Einsatz hostbasierter Analysetools
- Protokollierung der durchgeführten Analyseschritte
- Analyse des Netzwerkverkehrs und von Protokolldaten
- Berücksichtigung datenschutzrechtlicher Anforderungen im Rahmen der Durchführung o.g. Tätigkeiten
- Hostbasierte Suche (Scan-Tools, AV, ...)

Die Ausstattung muss die Analyse verschiedener Systeme ermöglichen, dabei sollten die aktuell gebräuchlichste Hardware sowie die aktuellen Betriebssysteme und Netzwerktechnologien abgedeckt werden.

**Hostbasierte Suche**
Der Dienstleister sollte über Fähigkeiten verfügen, hostbasierte Indikatoren in einem großen Netzwerk mit vielen Systemen suchen zu können. Idealerweise besitzt er bereits a priori vor dem APT-Vorfall einen großen Satz an generischen und gruppenspezifischen Indikatoren.

**Dokumentation**
Darüber hinaus sind vom kompromittierten Netz unabhängige Kommunikations- und Arbeitsmöglichkeiten mitzubringen. Hierzu gehören auch vorbereitete Dokumentationstools und Vorlagen. Diese müssen Schnittstellen für ggf. weitere, durch den Arbeitgeber bereitgestellte Teams haben.

# 3 Weiterführende Informationen

Die BSI-Empfehlung „Schützen Sie sich vor professionellen gezielten Cyber-Angriffen“[4] zeigt die Gefahren auf, welche durch professionelle Angreifer entstehen können, und behandelt mögliche Schutzmaßnahmen, um sich gegen diese Angriffe zu schützen.

Sollte der Verdacht auf einen APT-Angriff bestehen, stellt die BSI-Empfehlung „Erste Hilfe bei einem APT-Angriff“[5] ein Notfalldokument dar, welches von IT-Sicherheitsbeauftragten, CISOs und Systemadministratoren für erste Reaktionen genutzt werden kann.

4 https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_115.html
5 https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_072_TLP-White.html