Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Qualifizierte APT-Response Dienstleister

im Sinne § 3 BSIG

Stand: 28. März 2025

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582- 0
E-Mail: qdl@bsi.bund.de
Internet: https://www.bsi.bund.de

Inhalt

1 Hintergrund

Das BSI hat gemäß § 3 BSIG die Aufgabe, Betreiber Kritischer Infrastrukturen auf deren Ersuchen bei der Sicherung ihrer Informationstechnik zu beraten und zu unterstützen. Hierzu kann auch auf qualifizierte Sicherheitsdienstleister verwiesen werden.

Angriffe auf Unternehmen nehmen in der letzten Zeit stark zu, sowohl in der Anzahl, als auch in der Intensität der Bedrohungen. Der Schaden, welcher dabei entsteht, verursacht bei den betroffenen Unternehmen nicht nur große wirtschaftliche Schäden, sondern auch einen Reputationsverlust, wenn Dienste nicht zur Verfügung stehen oder ein Datenabfluss zu verzeichnen war. Zur Verbesserung der Abwehr oder zur Bewältigung eines erfolgreichen Angriffs bedarf es vielfältig der Unterstützung externer Dienstleister, die in ihrem jeweiligen Tätigkeitsgebiet ein hohes Spezialwissen erlangt haben.

Mit der Benennung von themenspezifischen Qualitätskriterien und der Identifikation geeigneter Dienstleister möchte das BSI betroffenen Unternehmen eine Hilfestellung bei der Suche und Auswahl geeigneter Dienstleister bieten, um die Unternehmen im Ernstfall von einem eigenen zeitintensiven Rechercheaufwand zu entlasten. Gleichzeitig soll auf diese Weise ein gewisses Qualitätsniveau in der jeweiligen Branche etabliert werden.

Zur Identifikation von qualifizierten Sicherheitsdienstleistern für die Abwehr von APT-Angriffen hat das BSI Kriterien[1] veröffentlicht, die betroffene Betreiber Kritischer Infrastrukturen bei der Auswahl von geeigneten Dienstleistern unterstützen sollen.

Die Dienstleister, die anhand der Kriterien mit der Hilfe des in Kapitel 2 beschriebenen Verfahrens gefunden wurden, sind in diesem Dokument im Folgenden aufgelistet. Dazu gehören sowohl die Kontaktdaten in Kapitel 3 als auch die Gegenüberstellung der einzelnen Leistungsmerkmale in Kapitel 5. Die Leistungsmerkmale, welche sowohl die Kriterien beinhalten als auch weitere individuelle Unterschiede der Dienstleister darstellen, werden zuvor in Kapitel 4 genauer beschrieben.

[1] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Auswahlkriterien_APT-Response_Dienstleister.html

2 Verfahren

Um den Betreibern Kritischer Infrastrukturen eine leichtere Übersicht über den Markt der APT-Response-Dienstleister zu bieten, wurde, basierend auf den Auswahlkriterien, ein Verfahren zur Identifizierung geeigneter Dienstleister durchgeführt.

Das Verfahren gliedert sich in die folgenden Schritte:

1. Überprüfung der vom Dienstleister bereitgestellten Dokumentation
   Der Dienstleister musste zunächst eine vollständige Dokumentation bereitstellen. Hierzu zählten sowohl Beschreibungen der Produkte und Dienstleistungen, als auch Erläuterungen in Bezug auf die Einhaltung der vom BSI aufgestellten Kriterien. Des Weiteren bestand die Möglichkeit, vorhandene Zertifizierungen von Rechenzentren oder dem Unternehmen selbst mitzuliefern.
2. Durchführung eines Fachinterviews
   In einem mehrstündigen Termin beim BSI musste der Dienstleister anhand fiktiver Szenarien zeigen, dass er in der Lage ist, die Situationen fach- und zielgerichtet zu bedienen. Dabei wurde sowohl auf das allgemeine Vorgehen des Dienstleisters, als auch auf gestellte Fragen und Verarbeitung der erhaltenen Informationen geachtet.

Weiteren interessierten Dienstleistern steht das Verfahren jederzeit offen, sie können sich für Informationen an das Funktionspostfach qdl@bsi.bund.de wenden.

3 Qualifizierte APT-Response-Dienstleister

Im Folgenden werden die bisher identifizierten qualifizierten APT-Response-Dienstleister mit den entsprechenden Kontaktdaten in alphabetischer Reihenfolge aufgelistet.

3.1 @-yet GmbH

Homepage	https://www.at-yet.de
Kontakt-Telefonnummer	+49 (0) 2175 1655 0
Kontakt-E-Mail-Adresse	notfall@at-yet.de

3.2 Airbus Protect GmbH

Homepage	https://www.protect.airbus.com/cyber-incident-response/
Kontakt-Telefonnummer	+49 16 03 21 61 84 +33 9 72 30 13 99
Kontakt-E-Mail-Adresse	acs-csirt-de@airbus.com

3.3 Antago GmbH

Homepage	https://antago.de/
Kontakt-Telefonnummer	+49 (0) 6251 86158 0
Kontakt-E-Mail-Adresse	incident@antago.de

3.4 Arctic Wolf Networks Germany GmbH

Homepage	https://arcticwolf.com/de/solutions/incident-response/
Kontakt-Telefonnummer	+49 (0) 30 16637144
Kontakt-E-Mail-Adresse	newcase@arcticwolf.com

3.5 BDO Cyber Security GmbH

Homepage	https://www.bdosecurity.de
Kontakt-Telefonnummer	+49 (0) 40 32890 6540
Kontakt-E-Mail-Adresse	circc@bdosecurity.de

3.6 Bechtle AG

Homepage	https://www.bechtle.com
Kontakt-Telefonnummer	+49 (0) 7132 981 2783
Kontakt-E-Mail-Adresse	help.sirt@bechtle.com

3.7 BFK edv-consulting GmbH

Homepage	https://www.bfk.de
Kontakt-Telefonnummer	+49 (0) 721 962011
Kontakt-E-Mail-Adresse	cfischer@bfk.de

3.8 BlackBerry Deutschland GmbH

Homepage	https://www.blackberry.com/de/de/services/blackberry-cybersecurity-consulting/overview
Kontakt-Telefonnummer	+49 (0) 800 2060 2065
Kontakt-E-Mail-Adresse	irretainer@blackberry.com

3.9 CERTAINITY Holding GmbH

Homepage	https://certainity.com/en/
Kontakt-Telefonnummer	+49 (0) 800 2378246 AUT: +43 664 88844686
Kontakt-E-Mail-Adresse	csirt@certainity.com

3.10 Cirosec GmbH

Homepage	https://www.cirosec.de
Kontakt-Telefonnummer	+49 (0) 7131 59455 0
Kontakt-E-Mail-Adresse	info@cirosec.de

3.11 Cisco Talos Incident Response

Homepage	https://talosintelligence.com/incident_response
Kontakt-Telefonnummer	+44 808 234 6353
Kontakt-E-Mail-Adresse	IncidentResponse@cisco.com

3.12 Code Blue GmbH

Homepage	https://codebluecyber.de/
Kontakt-Telefonnummer	+49 (0) 69 979 460-999
Kontakt-E-Mail-Adresse	notfall@codebluecyber.de

3.13 Corporate Trust Business Risk & Crisis Management GmbH

Homepage	https://www.corporate-trust.de
Kontakt-Telefonnummer	+49 (0) 89 599 88 75 80
Kontakt-E-Mail-Adresse	info@corporate-trust.de

3.14 CrowdStrike

Homepage	https://www.crowdstrike.de/gab-es-eine-sicherheitsverletzung/
Kontakt-Telefonnummer	+49 (0) 800 3252669
Kontakt-E-Mail-Adresse	services@crowdstrike.com

3.15 DCSO Deutsche Cyber-Sicherheitsorganisation GmbH

Homepage	https://dcso.de
Kontakt-Telefonnummer	+49 (0) 30 726219 0
Kontakt-E-Mail-Adresse	incident@dcso.de

3.16 Deloitte GmbH

Homepage	https://www.deloitte.com/de/de/services/risk-advisory/services/cyber-incident-response0.html
Kontakt-Telefonnummer	+49 (0) 40 32080 4499 (englischsprachige Hotline)
Kontakt-E-Mail-Adresse	csirt@deloitte.de

3.17 Deutsche Telekom Security GmbH

Ansprechpartner	Malte Fiedler
Homepage	https://geschaeftskunden.telekom.de/digitale-loesungen/cyber-security
Kontakt-Telefonnummer	+49 (0) 170 3278537
Kontakt-E-Mail-Adresse	Pentesting+IRS@t-systems.com

3.18 DigiFors GmbH

Homepage	https://digifors.de
Kontakt-Telefonnummer	+49 (0) 0341 6567 3381
Kontakt-E-Mail-Adresse	notfall@digifors.de

3.19 Dr. Michael Gorski Consulting GmbH

Homepage	https://www.michaelgorski.net/
Kontakt-Telefonnummer	+49 (0)2173 9998710
Kontakt-E-Mail-Adresse	soc@michaelgorski.net

3.20 ERNW Research GmbH

Homepage	https://www.ernw-research.de
Kontakt-Telefonnummer	+49 (0) 6221 7569637
Kontakt-E-Mail-Adresse	incident-response@ernw.de

3.21 ETAS GmbH

Homepage	https://www.etas.com/de/portfolio/incident-response-as-a-service.php
Kontakt-Telefonnummer	+49 (0) 234 43870-200
Kontakt-E-Mail-Adresse	incident@escrypt.com

3.22 EY GmbH & Co. KG Wirtschaftsprüfungsgesellschaft

Homepage	https://www.ey.com/de_de/assurance/privacy-cyber-response
Kontakt-Telefonnummer	+49 (0) 800 2323273
Kontakt-E-Mail-Adresse	ir@de.ey.com

3.23 Eye Security GmbH

Homepage	https://www.eye.security/de/
Kontakt-Telefonnummer	+49 (0)203 6688 1900
Kontakt-E-Mail-Adresse	cert@eye.security

3.24 GDATA Advanced Analytics GmbH

Homepage	https://www.gdata-advancedanalytics.de
Kontakt-Telefonnummer	+49 (0) 234 9762 800
Kontakt-E-Mail-Adresse	info@gdata-adan.de

3.25 glueckkanja AG

Homepage	https://www.glueckkanja.com
Kontakt-Telefonnummer	+49 (0) 1805009823
Kontakt-E-Mail-Adresse	apt@glueckkanja.com

3.26 Grant Thornton AG Wirtschaftsprüfungsgesellschaft

Homepage	https://www.grantthornton.de/services/cyber-security/
Kontakt-Telefonnummer	+49 (0) 211 9524-3347
Kontakt-E-Mail-Adresse	CIR@de.gt.com

3.27 HiSolutions AG

Homepage	https://www.hisolutions.com
Kontakt-Telefonnummer	+49 (0) 30 533289 0
Kontakt-E-Mail-Adresse	info@hisolutions.com

3.28 HvS-Consulting GmbH

Homepage	https://www.hvs-consulting.de/de/incident-response/
Kontakt-Telefonnummer	+49 (0) 89 890 636 261
Kontakt-E-Mail-Adresse	incidentresponse@hvs-consulting.de

3.29 intersoft consulting services AG

Homepage	https://www.intersoft-consulting.de	
Kontakt-Telefonnummer	zu normalen Geschäftszeiten 24/7 Hotline	+49 (0) 40 790 235 0 +49 (0) 180 622 124 6
Kontakt-E-Mail-Adresse	it-forensik@intersoft-consulting.de	

3.30 InfoGuard AG

Homepage	https://www.infoguard.de/incident-response
Kontakt-Telefonnummer	+49 (0) 896 282-5265
Kontakt-E-Mail-Adresse	investigations@infoguard.de

3.31 IS4IT GmbH

Homepage	https://www.is4it.de
Kontakt-Telefonnummer	+49 (0) 89 638 98 48-0 +49 (0) 711 490 962-0
Kontakt-E-Mail-Adresse	csirt@is4it.de

3.32 KPMG AG Wirtschaftsprüfungsgesellschaft

Homepage	https://home.kpmg/de/de/home/dienstleistungen/audit/forensic/cyber-incident-response-investigation.html	
Kontakt-Telefonnummer	innerhalb Deutschlands außerhalb Deutschlands	+49 (0) 800 767 5764 +49 202 251557146
Kontakt-E-Mail-Adresse	de-sos@kpmg.com	

3.33 LEITWERK AG

Homepage	https://www.leitwerk.de
Kontakt-Telefonnummer	+49 (0) 7805 918 112
Kontakt-E-Mail-Adresse	support@leitwerk.de

3.34 Mandiant Deutschland GmbH

Homepage	https://www.mandiant.com
Kontakt-Telefonnummer	+49 (0) 800 181 7231
Kontakt-E-Mail-Adresse	investigations@mandiant.com

3.35 Microsoft Deutschland GmbH

Homepage	https://www.microsoft.com/security
Kontakt-Telefonnummer	+49 (0) 89 23 129 129
Kontakt-E-Mail-Adresse	https://aka.ms/serviceshub

3.36 msg systems ag - security advisors

Homepage	https://security-advisors.msg.group
Kontakt-Telefonnummer	+49 (0) 89 95469587
Kontakt-E-Mail-Adresse	dfir@msg.group

3.37 NCC Group GmbH

Homepage	https://www.nccgroup.com	
Kontakt-Telefonnummer	24/7 Hotline Telefon Zentrale	+49 (0) 89 2019 0489 +49 (0) 89 599 762 0
Kontakt-E-Mail-Adresse	michiel.renzenbrink@nccgroup.com	

3.38 Northwave

Homepage	https://www.northwave-security.com
Kontakt-Telefonnummer	+ 31 85 043 7909
Kontakt-E-Mail-Adresse	info@northwave-security.com

3.39 NVISO GmbH

Homepage	https://www.nviso.eu/de
Kontakt-Telefonnummer	+49 (0) 69 8088 3829
Kontakt-E-Mail-Adresse	csirt@nviso.de

3.40 Oneconsult Deutschland AG

Homepage	https://www.oneconsult.com/
Kontakt-Telefonnummer	DE: +49 89 248 820 690 CH: +41 43 377 22 90
Kontakt-E-Mail-Adresse	csirt@oneconsult.com

3.41 Orange Cyberdefense Germany GmbH

Homepage	www.orangecyberdefense.com
Kontakt-Telefonnummer	+49 (0) 821 808 30 470
Kontakt-E-Mail-Adresse	CSIRT@orangecyberdefense.com

3.42 Palo Alto Networks

Homepage	https://unit42.paloaltonetworks.com/
Kontakt-Telefonnummer	+31202993130
Kontakt-E-Mail-Adresse	unit42-investigations@paloaltonetworks.com

3.43 pco GmbH & Co. KG.

Homepage	https://www.pco-online.de

Kontakt-Telefonnummer +49 541 9632 5201

Kontakt-E-Mail-Adresse support@pco-online.de

3.44 PricewaterhouseCoopers GmbH Wirtschaftsprüfungsgesellschaft

Homepage https://pwc.de

https://www.pwc.de/de/im-fokus/cyber-security/cyber-incident-response.html

Kontakt-Telefonnummer +49 (0) 69 9585 9992

Kontakt-E-Mail-Adresse de_sir@pwc.com

3.45 QGroup GmbH

Homepage https://www.qgroup.de

Kontakt-Telefonnummer +49 (0) 69 175363-047

Kontakt-E-Mail-Adresse emergency@qgroup.de

3.46 Rapid7 Germany GmbH

Homepage https://www.rapid7.com/

Kontakt-Telefonnummer +1 844 727 4347

Kontakt-E-Mail-Adresse sales-dach@rapid7.com

3.47 r-tec IT Security GmbH

Homepage https://www.r-tec.net/incident-response-service.html

Kontakt-Telefonnummer +49 (0) 202 31767-112

Kontakt-E-Mail-Adresse incident-response@r-tec.net

3.48 SEC Consult Unternehmensberatung GmbH

Homepage https://sec-consult.com/de/incident-response/sec-defence/

Kontakt-Telefonnummer +49 (0) 30 398 2027 77

Kontakt-E-Mail-Adresse secdefence@sec-consult.com

3.49 SECUINFRA GmbH

Homepage https://www.secuinfra.com

Kontakt-Telefonnummer +49 (0) 30 555 702 112

Kontakt-E-Mail-Adresse forensik@secuinfra.com

incident@secuinfra.com

3.50 Sophos Technology GmbH

Homepage	https://www.sophos.de/rapid-response
Kontakt-Telefonnummer	+49 (0) 611 7118 6766
Kontakt-E-Mail-Adresse	RapidResponse@sophos.com

3.51 SVA System Vertrieb Alexander GmbH

Homepage	https://www.sva.de
Kontakt-Telefonnummer	+49 (0) 6122 95092 92
Kontakt-E-Mail-Adresse	incident-response@sva.de

3.52 SySS GmbH

Homepage	https://www.syss.de
Kontakt-Telefonnummer	+49 (0) 7071 407856 40
Kontakt-E-Mail-Adresse	csrit@syss.de

3.53 Trend Micro Incident Response

Homepage	https://www.trendmicro.com/
Kontakt-Telefonnummer	+49 (0) 89 54198959
Kontakt-E-Mail-Adresse	incident_response@trendmicro.com

3.54 Verizon Deutschland GmbH

Ansprechpartner	Stefan Englbrecht
Homepage	https://www.verizon.com/business/de-de/products/security/
Kontakt-Telefonnummer	00 - 80085757575
Kontakt-E-Mail-Adresse	ir-hotline@verizon.com

3.55 Wipro

Homepage	www.wipro.com
Kontakt-Telefonnummer	Jeff Hamm: +49 (0) 162 2831672 Holger Wilken: +49 (0) 151 61 888 928
Kontakt-E-Mail-Adresse	jeff.hamm@wipro.com holger.wilken@wipro.com

3.56 WithSecure GmbH

Homepage	https://www.withsecure.com/de/home
Kontakt-Telefonnummer	+49 (0) 891 2086 531
Kontakt-E-Mail-Adresse	mdr-dach@withsecure.com

4 Leistungsmerkmale

4.1 24x7 Erreichbarkeit

Ist der APT-Response-Dienstleister rund um die Uhr bei Angriffen oder Problemen erreichbar? Dies kann insbesondere für erste Einschätzungen notwendig sein.

4.2 ISO27001-Zertifizierung der Institution

Besitzt der APT-Response-Dienstleister eine ISO27001 Zertifizierung für die Institution?

4.3 Hauptsitz des Dienstleisters in der EU

Befindet sich der Hauptsitz des Dienstleisters in einem Land der Europäischen Union?

4.4 Sichere Aufbewahrungsmöglichkeiten

Während der Bearbeitung des APT-Vorfalls fallen verschiedene Daten an. Dazu gehören zum Beispiel Dokumentationen, Log-Dateien oder Festplattenkopien. Diese können zum Teil vertrauliche Daten enthalten, welche auch beim Dienstleister entsprechend geschützt werden müssen.

4.5 APT-Dienstleistungen durch eigene Mitarbeitende

Bei der Aufarbeitung eines APT-Vorfalls werden viele verschiedene Kenntnisse benötigt, welche auch in den veröffentlichten Kriterien[2] aufgeführt sind. Teilweise greifen die Dienstleister dabei auch auf externe Unterstützung zurück, sodass keine eigenen Kenntnisse vorhanden sind.

Die Definitionen der einzelnen Rollen und Themenbereiche sind in den veröffentlichten Kriterien[2] zu finden.

4.5.1 Ermittlungsleitung

4.5.2 Malware-Analyse

4.5.3 Host-Forensik

4.5.4 Netzwerkforensik

4.6 Weitere Dienstleistungsangebote

4.6.1 Beratung durch Dienstleister-eigene Juristen

Da bei der Bearbeitung eines APT-Vorfalls auch zahlreiche juristische Fragen geklärt werden müssen, ist die Hilfe von Juristen in den meisten Fällen zwingend notwendig. Falls der qualifizierte Dienstleister eigene Juristen für solche Fälle beschäftigt, können diese hinzugezogen werden.

4.6.2 Krisenkommunikation

Bei einem APT-Vorfall muss häufig eine Strategie für den öffentlichen Umgang entwickelt und umgesetzt werden. Dabei kann, falls möglich der qualifizierte Dienstleister unterstützen.

[2] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Auswahlkriterien_APT-Response_Dienstleister.html

4.6.3 Durchführung des Wiederaufbaus der Systeme

Nachdem der APT-Vorfall abschließend untersucht wurde, müssen mindestens die betroffenen Systeme bereinigt und neu aufgesetzt werden. Dies kann möglicherweise durch den qualifizierten Dienstleister erfolgen, falls dieser die Dienstleistung ebenfalls anbietet.

4.7 Technische Ausstattung

4.7.1 Fähigkeit zur Malware-Analyse

Verfügt der Dienstleister über die notwendigen technischen Voraussetzungen zur Analyse von Malware?

Dazu gehört zum Beispiel ein Labor mit der Möglichkeit, Malware in einer geschützten Umgebung auszuführen (dynamische Analyse) sowie durch Reverse Engineering (Disassemblierung, statische Analyse) zu analysieren.

4.7.2 Mobil einsetzbare Ausstattung

Verfügt der Dienstleister über die notwendigen technischen Voraussetzungen zur Durchführung von forensischen Untersuchungen bei dem Auftraggeber vor Ort?

Dazu gehört mindestens eine ausreichende mobile Ausstattung, um die Datenakquise vor Ort durchführen zu können.

4.7.3 Hostbasierte Suche

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

5 Gegenüberstellung der Leistungsmerkmale der einzelnen APT-Response-Dienstleister

					4.5 APT-Dienstleistungen durch eigene Mitarbeitende				4.6 Weitere Dienstleistungsangebote			4.7 Technische Ausstattung		
	4.1 24x7 Erreichbarkeit	4.2 ISO27001-Zertifizierung der Institution	4.3 Hauptsitz des Dienstleisters in der EU	4.4 Sichere Aufbewahrungsmöglichkeiten	4.5.1 Ermittlungsleitung	4.5.2 Malware-Analyse	4.5.3 Host-Forensik	4.5.4 Netzwerkforensik	4.6.1 Beratung durch Dienstleister-eigene Juristen	4.6.2 Krisenkommunikation	4.6.3 Durchführung des Wiederaufbaus der Systeme	4.7.1 Fähigkeit zur Malware-Analyse	4.7.2 Mobil einsetzbare Ausstattung	4.7.3 Hostbasierte Suche
@-yet GmbH	+[a]	+	+	+	+	+	+	+	+	+	+	+	+	+
Airbus Protect GmbH	+	+	+	+	+	+	+	+	–[b]	+	+	+	+	+
Antago GmbH	–	+	+	+	+	+	+	+	–[b]	–	–[c]	+	+	+
Arctic Wolf Networks Germany GmbH	+	+	+	+	+	+	+	+	–	–	+[d]	+	+	+
BDO Cyber Security GmbH	+	+	+	+	+	+	+	+	+[e]	+	–[f]	+	+	+
Bechtle AG	+	+	+	+	+	+	+	+	–	+	+	+	+	+
BFK edv-consulting GmbH	+	–	+	+	+	+	+	+	–[b]	+	–[c]	+	+	+
BlackBerry Deutschland GmbH	+	+	+	+	+	+	+	+	+[b]	–[b]	–[c]	+	+	+

					4.5 APT-Dienstleistungen durch eigene Mitarbeitende				4.6 Weitere Dienstleistungsangebote			4.7 Technische Ausstattung		
	4.1 24x7 Erreichbarkeit	4.2 ISO27001-Zertifizierung der Institution	4.3 Hauptsitz des Dienstleisters in der EU	4.4 Sichere Aufbewahrungsmöglichkeiten	4.5.1 Ermittlungsleitung	4.5.2 Malware-Analyse	4.5.3 Host-Forensik	4.5.4 Netzwerkforensik	4.6.1 Beratung durch Dienstleister-eigene Juristen	4.6.2 Krisenkommunikation	4.6.3 Durchführung des Wiederaufbaus der Systeme	4.7.1 Fähigkeit zur Malware-Analyse	4.7.2 Mobil einsetzbare Ausstattung	4.7.3 Hostbasierte Suche
CERTAINITY Holding GmbH	+	–[g]	+	+	+	+	+	+	–[b]	–[b]	+	+	+	+
Cirosec GmbH	+[a]	+	+	+	+	+	+	+	–[b]	–[b]	–[c]	+	+	+
Cisco Talos Incident Response	+	+	+	+	+	+	+	+	–	+	–[c]	+	+	+
Code Blue GmbH	+	–	+	+	+	+	+	+	–[b]	+	–[i]	+	+	+
Corporate Trust	+[a]	–	+	+	+	+[h]	+	+	–[b]	+	–[c]	+[h]	+	+
CrowdStrike	+	+	+	+	+	+	+	+	–	–[i]	+	+	+	+
DCSO	+	+	+	+	+	+	+	+	–	–	–[c]	+	+	+
Deloitte GmbH	+[a]	+	+	+	+	+	+	+	+	–[b]	+	+	+	+
DigiFors GmbH	+	+	+	+	+	+	+	+	–[b]	–[b]	–[c]	+	+	+
Dr. Michael Gorski Consulting GmbH	+	–	+	–	+	+	+	+	–[b]	+	–[c]	+	+	+

					4.5 APT-Dienstleistungen durch eigene Mitarbeitende				4.6 Weitere Dienstleistungsangebote			4.7 Technische Ausstattung		
	4.1 24x7 Erreichbarkeit	4.2 ISO27001-Zertifizierung der Institution	4.3 Hauptsitz des Dienstleisters in der EU	4.4 Sichere Aufbewahrungsmöglichkeiten	4.5.1 Ermittlungsleitung	4.5.2 Malware-Analyse	4.5.3 Host-Forensik	4.5.4 Netzwerkforensik	4.6.1 Beratung durch Dienstleister-eigene Juristen	4.6.2 Krisenkommunikation	4.6.3 Durchführung des Wiederaufbaus der Systeme	4.7.1 Fähigkeit zur Malware-Analyse	4.7.2 Mobil einsetzbare Ausstattung	4.7.3 Hostbasierte Suche
EY GmbH & Co. KG Wirtschaftsprüfungsgesellschaft	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ERNW Research GmbH	+	-	+	+	+	+	+	+	-	-b	+j	+	+	+
ETAS GmbH	+a	-	+	+	+	+	+	+	-b	-b	-c	+	+	+
Eye Security GmbH	+	+	+	+	+	+	+	+	-b	+	-i	+	+	+
GDATA Advanced Analytics	+	-	+	+	+	+	+	+	-b	-b	-c	+	+	+
glueckkanja AG	+	+	+	+	+	+	+	+	-b	-	+	+	-	+
Grant Thornton AG	+	+	+	+	+	+h	+	+	+	+	-c	+h	+	-
HiSolutions AG	+a	+	+	+	+	+	+	+	-b	+	-c	+	+	+
HvS-Consulting GmbH	+a	-	+	+	+	+	+	+	-b	-b	-c	+	+	+
InfoGuard AG	+	+	-	+	+	+	+	+	+	+	+	+	+	+

					4.5 APT-Dienstleistungen durch eigene Mitarbeitende				4.6 Weitere Dienstleistungsangebote			4.7 Technische Ausstattung		
	4.1 24x7 Erreichbarkeit	4.2 ISO27001-Zertifizierung der Institution	4.3 Hauptsitz des Dienstleisters in der EU	4.4 Sichere Aufbewahrungsmöglichkeit en	4.5.1 Ermittlungsleitung	4.5.2 Malware-Analyse	4.5.3 Host-Forensik	4.5.4 Netzwerkforensik	4.6.1 Beratung durch Dienstleister-eigene Juristen	4.6.2 Krisenkommunikation	4.6.3 Durchführung des Wiederaufbaus der Systeme	4.7.1 Fähigkeit zur Malware-Analyse	4.7.2 Mobil einsetzbare Ausstattung	4.7.3 Hostbasierte Suche
intersoft consulting services AG	+	+	+	+	+	+	+	+	+	+	+[j]	+	+	+
IS4IT GmbH	+[a]	+	+	+	+	+	+	+	-	+[k]	+	+	+	+
KPMG AG	+	+	+	+	+	+	+	+	+	+	-[c]	+	+	+
LEITWERK AG	+	+	+	+	+	+	+	+	-	+	+	+	+	+
Mandiant Deutschland GmbH	+	-	+	+	+	+	+	+	-[b]	+	-[c]	+	+	+
Microsoft Deutschland GmbH	+	+	-	+[a]	+	+	+	+	-	+	+	+	+	+
msg systems ag - security advisors	+	+	+	+	+	+	+	+	-	+	+	+	+	+
NCC Group GmbH	+	+	+	+	+	+	+	+	+	+	+	+	+	+
Northwave	+	+	+	+	+	+	+	+	-	-[i]	+	+	+	+
NVISO GmbH	+	+	+	+	+	+	+	+	-	-[i]	-[c]	+	+	+

					4.5 APT-Dienstleistungen durch eigene Mitarbeitende				4.6 Weitere Dienstleistungsangebote			4.7 Technische Ausstattung		
	4.1 24x7 Erreichbarkeit	4.2 ISO27001-Zertifizierung der Institution	4.3 Hauptsitz des Dienstleisters in der EU	4.4 Sichere Aufbewahrungsmöglichkeiten	4.5.1 Ermittlungsleitung	4.5.2 Malware-Analyse	4.5.3 Host-Forensik	4.5.4 Netzwerkforensik	4.6.1 Beratung durch Dienstleister-eigene Juristen	4.6.2 Krisenkommunikation	4.6.3 Durchführung des Wiederaufbaus der Systeme	4.7.1 Fähigkeit zur Malware-Analyse	4.7.2 Mobil einsetzbare Ausstattung	4.7.3 Hostbasierte Suche
Oneconsult Deutschland AG	+	+	+	+	+	+	+	+	+	−[b]	−[i]	+	+	+
Orange Cyberdefense Germany GmbH	+	+	+	+	+	+	+	+	-	+	-	+	+	+
Palo Alto Networks	+	+	+	+	+	+	+	+	−[b]	−[b]	−[c]	+	+	+
pco GmbH & Co. KG	+[a]	+	+	+	+	+	+	+	+	-	+	+	+	+
PricewaterhouseCoopers GmbH	+	+	+	+	+	+	+	+	+	+	−[c]	+	+	+
QGroup	+	−[l]	+	+	+	+	+	+	-	−[i]	−[c]	+	+	+
Rapid7 Germany GmbH	−[a]	+	+	+	+	+	+	+	-	+	−[i]	+	-	+
r-tec IT Security GmbH	+[a]	+	+	+	+	+	+	+	−[b]	−[b]	+	+	+	+
SEC Consult	+	+	+	+	+	+	+	+	-	+	+	+	+	+
SECUINFRA GmbH	+	+	+	+	+	+	+	+	-	−[b]	+	+	+	+

					4.5 APT-Dienstleistungen durch eigene Mitarbeitende				4.6 Weitere Dienstleistungsangebote			4.7 Technische Ausstattung		
	4.1 24x7 Erreichbarkeit	4.2 ISO27001-Zertifizierung der Institution	4.3 Hauptsitz des Dienstleisters in der EU	4.4 Sichere Aufbewahrungsmöglichkeiten	4.5.1 Ermittlungsleitung	4.5.2 Malware-Analyse	4.5.3 Host-Forensik	4.5.4 Netzwerkforensik	4.6.1 Beratung durch Dienstleister-eigene Juristen	4.6.2 Krisenkommunikation	4.6.3 Durchführung des Wiederaufbaus der Systeme	4.7.1 Fähigkeit zur Malware-Analyse	4.7.2 Mobil einsetzbare Ausstattung	4.7.3 Hostbasierte Suche
Sophos Technology GmbH	+	+	+	+	+	+	+	+	-	-[i]	-[c]	+	+	+
SVA	+[a]	+	+	+	+	+	+	+	-	+	+	+	+	+
SySS GmbH	+	+	+	+	+	+	+	+	-	-	-[c]	+	+	+
Trend Micro Incident Response	+	+	+	+	+	+	+	+	-	-	-[c]	+	+	+
Telekom Security	+	+	+	+	+	+	+	+	-	+	+	+	+	+
Verizon Deutschland GmbH	+	+	+	+	+	+	+	+	-[b]	+	-[i]	+	+	+
Wipro	+	+	+	+	+	+	+	+	+	+	-	+	+	+
WithSecure GmbH	+	+	+	+	+	+	+	+	-	-	-	+	+	+

[a] Nach entsprechender Vereinbarung
[b] In Zusammenarbeit mit externen Partnerunternehmen

[c] Externes Systemhaus wird vom Dienstleister begleitet und beraten
[d] Ergänzend mit externen Partnerunternehmen
[e] In Zusammenarbeit mit internem Partnerunternehmen.
[f] Internes Partnerunternehmen wird beraten und unterstützt.
[g] Ist in Vorbereitung
[h] Bei umfangreichen Analysen in Zusammenarbeit mit einem externen Partnerunternehmen
[i] Unterstützung und fachliche Beratung wird angeboten
[j] Wiederaufbau erfolgt bei KMUs oder beim Thema Active Directory selbst, ansonsten wird externes Systemhaus vom Dienstleister begleitet und beraten
[k] Bei umfangreichen Vorfällen in Zusammenarbeit mit externem Partnerunternehmen
[l] In Erstellung