Bundesamt
für Sicherheit in der
Informationstechnik

Qualifizierte APT-Response Dienstleister

im Sinne § 3 BSIG

Stand: 24. Mai 2019

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
© Bundesamt für Sicherheit in der Informationstechnik 2018

Inhaltsverzeichnis

1 Hintergrund ... 5
2 Verfahren ... 6
3 Qualifizierte APT-Response-Dienstleister ... 7
3.1 BFK edv-consulting GmbH ... 7
3.2 DCSO Deutsche Cyber-Sicherheitsorganisation GmbH ... 7
3.3 HiSolutions AG ... 7
3.4 QuoScient GmbH ... 7
3.5 SySS GmbH ... 7
3.6 T-Systems International GmbH – Telekom Security ... 7
3.7 Warth & Klein Grant Thornton AG Wirtschaftsprüfungsgesellschaft ... 8
4 Leistungsmerkmale ... 9
4.1 24x7 Erreichbarkeit ... 9
4.2 ISO27001-Zertifizierung der Institution ... 9
4.3 Hauptsitz des Dienstleisters in der EU ... 9
4.4 Sichere Aufbewahrungsmöglichkeiten ... 9
4.5 APT-Dienstleistungen durch eigene Mitarbeiter ... 9
4.6 Weitere Dienstleistungsangebote ... 9
4.7 Technische Ausstattung ... 10
5 Gegenüberstellung der Leistungsmerkmale der einzelnen APT-Response-Dienstleister ... 11

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 betroffenene 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 BFK edv-consulting GmbH

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

3.2 DCSO Deutsche Cyber-Sicherheitsorganisation GmbH

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

3.3 HiSolutions AG

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

3.4 QuoScient GmbH

Homepage	https://www.quoscient.io/de/
Kontakt-Telefonnummer	+49 (0)69 56608909
Kontakt-E-Mail-Adresse	Threat-Ops@quoscient.io

3.5 SySS GmbH

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

3.6 T-Systems International GmbH – Telekom Security

Homepage	https://www.t-systems.de/ict-security
Kontakt-Telefonnummer	+49 (0)89 545506105
Kontakt-E-Mail-Adresse	alexander.schinner@t-systems.com

3.7 Warth & Klein Grant Thornton AG Wirtschaftsprüfungsgesellschaft

Homepage	https://www.wkgt.com/services/governance-risk-compliance/
Kontakt-Telefonnummer	+49 (0)211 9524 8824
Kontakt-E-Mail-Adresse	helmut.brechtken@wkgt.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 Mitarbeiter

Bei der Aufarbeitung eines APT-Vorfalls werden viele verschiedene Kenntnisse benötigt, welche auch in den veröffentlichten Kriterien[1] 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[1] 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.

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

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

Die folgende Tabelle liefert eine grobe Gegenüberstellung einzelner Leistungsmerkmale der APT-Response-Dienstleister und soll einen ersten Ansatzpunkt für die Auswahl eines geeigneten Dienstleisters darstellen. Genauere Informationen können nur im Gespräch mit potentiell geeigneten Kandidaten erörtert werden.

Leistungsmerkmale	BFK edv-consulting GmbH	DCSO	HiSolutions AG	QuoScient GmbH	SySS GmbH	Telekom Security	WKGT
4.1 24x7 Erreichbarkeit	√	√	√[2]	√	√	√	√
4.2 ISO27001-Zertifizierung der Institution	X	X[3]	√	X	X[3]	√	X[3]
4.3 Hauptsitz des Dienstleisters in der EU	√	√	√	√	√	√	√
4.4 Sichere Aufbewahrungsmöglichkeiten	√	√	√	√	√	√	√
4.5 APT-Dienstleistungen durch eigene Mitarbeiter							
4.5.1 Ermittlungsleitung	√	√	√	√	√	√	√
4.5.2 Malware-Analyse	√	√	√	√	√	√	√[4]
4.5.3 Host-Forensik	√	√	√	√[5]	√	√	√

2 Nach entsprechender Vereinbarung
3 In Erstellung
4 Bei umfangreichen Analysen in Zusammenarbeit mit einem externen Partner
5 Unterstützung wird nur bei sehr vielen betroffenen Systemen hinzugezogen

Leistungsmerkmale	BFK edv-consulting GmbH	DCSO	HiSolutions AG	QuoScient GmbH	SySS GmbH	Telekom Security	WKGT
4.5.4 Netzwerkforensik	√	√	√	√	√	√	√
4.6 Weitere Dienstleistungsangebote							
4.6.1 Beratung durch Dienstleister-eigene Juristen	X[6]	X	X[6]	X[6]	X	X	√
4.6.2 Krisenkommunikation	√	X	X[6]	X[6]	X	√	√
4.6.3 Durchführung des Wiederaufbaus der Systeme	X[7]	X[7]	X[7]	X[7]	X[7]	√	X[7]
4.7 Technische Ausstattung							
4.7.1 Fähigkeit zur Malware-Analyse	√	√	√	√	√	√	√[8]
4.7.2 Mobil einsetzbare Ausstattung	√	√	√	√	√	√	√
4.7.3 Hostbasierte Suche	√	√	√	√	√	√	X

6 In Zusammenarbeit mit externen Partnern
7 Externes Systemhaus wird vom Dienstleister begleitet und beraten
8 Bei umfangreichen Analysen in Zusammenarbeit mit einem externen Partner