TLP:WHITE

Bundesamt
für Sicherheit in der
Informationstechnik

Advanced Persistent Threats

Teil 4 Reaktion
Technische und organisatorische Maßnahmen für die Vorfallsbearbeitung

Anlassbezogene und akute Hilfestellungen

Änderungshistorie

Version	*Datum*	*Name*	*Beschreibung*
Initiale Version v1.0	06.05.2020	Letitia Kernschmidt, Dr. Timo Steffens, Michael Dwucet	Konsolidierte und überarbeitete Fassung aller bestehenden Dokumente
v.1.1	08.05.2020	Letitia Kernschmidt	Aktualisierung eines Links
v2.0	26.06.2020	Letitia Kernschmidt	Neue Titel für alle APT-Dokumente, neue Anhänge und diverse Änderungen
v2.1	29.01.2020	Letitia Kernschmidt	URL Updates
v2.2	10.03.2021	Letitia Kernschmidt	URL Updates

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Internet: https://www.bsi.bund.de

Service-Center (Telefon): 0800 2741000
Service-Center (E-Mail): service-center@bsi.bund.de
Einen Vorfall melden: https://www.allianz-fuer-cybersicherheit.de/Webs/ACS/DE/IT-Sicherheitsvorfall/Unternehmen/Online-Meldung/online-meldung_node.html

Für die Zielgruppen und Partner des BSI gelten darüber hinaus die üblichen Meldewege.

Inhalt

1 Vorbemerkungen 4
2 Einleitung 5
2.1 Definition 5
3 Literaturverzeichnis 7

1 Vorbemerkungen

Dieses Dokument behandelt das Themengebiet **Reaktion bei APT-Angriffen**. Es richtet sich an **Systemadministratoren**, **IT-SiBe, CISOs, Leiter der IT, etc.** in Unternehmen und betrachtet daher eher **technische und organisatorische** Aspekte.

Ziel dieses Dokuments ist es, anlassbezogen akute und schnelle Hilfestellungen zu geben, die bei der Bearbeitung eines IT-Sicherheitsvorfalls dienlich sein können. Grundlage des Dokuments sind vor allem die vielfältigen und langjährigen Erfahrungen des BSI bei der Unterstützung von nationalen und internationalen Unternehmen und Institutionen bei der Vorfallsbearbeitung.

Das Dokument erhebt keinen Anspruch auf Vollständigkeit und soll nur als „Erste Hilfe“ und nicht als ganzheitliches Sicherheitskonzept verstanden werden. Naturgemäß überlappen sich Inhalte mit anderen BSI-Empfehlungen (z. B. dem IT-Grundschutz-Kompendium des BSI, vgl. [BSI2019a]); in diesem Dokument sind solche Inhalte aus anderen Empfehlungen enthalten, die anlassbezogen kurzfristig und prioritär umsetzbar sind.

Es sollte jedoch nicht unterschätzt werden, wie viel Zeit Sie für die Vorfallsbewältigung und die Umsetzung der genannten Maßnahmen brauchen. Grundsätzlich sollten Sie hier eher mit Wochen (und Monaten) als mit Tagen rechnen!

Das Dokument ist nach einem allgemeinen, einführenden Teil in einzelne Module unterteilt, die in sich geschlossen jeweils einen Themenkomplex behandeln. So können je nach Anwendungsfall die erforderlichen Informationen schnell und kompakt gefunden werden. Das Dokument beinhaltet die folgenden Module:

1. TLP:AMBER **Modul 1: Incident Response**
2. TLP:WHITE **Modul 2: Incident Management**
3. TLP:AMBER **Modul 3: Technische Analyse**

Folgende Symbole werden in diesem Dokument verwendet:

ⓘ Es folgt eine Kurzinformation zu dem Modul oder Abschnitt

Es folgt ein wichtiger Hinweis

Es folgt eine unbedingt zu beachtende Warnung

Der markierte Begriff wird in dem Glossar des Moduls näher erläutert

2 Einleitung

Grundsätzlich stellen gezielte IT-Angriffe für jede Behörde und jedes Unternehmen, das vertrauliche, geschäftskritische Informationen auf IT-Systemen verarbeitet oder dessen Erfolg (Gewinn und Umsatz) von der Verfügbarkeit seiner IT-Systeme abhängt, eine Bedrohung dar. In der Wirtschaft stehen Betriebs- und Geschäftsgeheimnisse, wie beispielsweise technologische Forschungs- und Entwicklungsergebnisse, Herstellungsverfahren oder unternehmenspolitische und operativ-betriebswirtschaftliche Entscheidungen wie Fusionen oder Verkäufe im Fokus der Angreifenden. In der öffentlichen Verwaltung sind es vor allem politische und wirtschaftliche Entscheidungen, deren vorzeitige Kenntnis zum eigenen Vorteil der Angreifenden oder zum Nachteil Dritter missbraucht werden können. Angegriffen werden aber nicht nur Behörden oder bekannte Großunternehmen, sondern auch klein- und mittelständische Unternehmen (KMU), die beispielsweise in ihrem Marktsegment eine herausragende Position einnehmen (Hidden Champions) oder die Rolle eines wichtigen Zulieferers oder IT-Dienstleisters für die zuvor genannten Großunternehmen innehaben. Dieser Einfallsvektor dient den Angreifern dann u.U. als Sprungbrett bzw. Multiplikator, wodurch sich ihnen weitere Angriffsmöglichkeiten bieten.

2.1 Definition

Im Zusammenhang mit professionellen gezielten Cyber-Angriffen hat sich der Begriff des **Advanced Persistent Threat (APT)** eingebürgert, der für eine spezielle Angriffsmethodik bzw. Motivation der Angreifenden steht. Obwohl die Begriffe APT und gezielter Angriff häufig synonym verwendet werden, handelt es sich, genau genommen, bei letzterem aber um einen Oberbegriff. Ein APT ist ein Spezialfall eines gezielten Angriffs und unterscheidet sich durch Methodik, Motivation und Angriffsziel von anderen gezielten Angriffen (z.B. Hacktivismus oder Angriffe auf einzelne Rechner). So beschreibt etwa der bekannte US-amerikanische IT-Sicherheitsexperte Bruce Schneier APTs wie folgt [Sch2011]:

> *„A conventional hacker or criminal isn't interested in any particular target. He wants a thousand credit card numbers for fraud, or to break into an account and turn it into a zombie, or whatever. Security against this sort of attacker is relative; as long as you're more secure than almost everyone else, the attackers will go after other people, not you. An APT is different; it's an attacker who - for whatever reason - wants to attack you. Against this sort of attacker, the absolute level of your security is what's important. It doesn't matter how secure you are compared to your peers; all that matters is whether you're secure enough to keep him out. APT attackers are more highly motivated. They're likely to be better skilled, better funded, and more patient. They're likely to try several different avenues of attack. And they're much more likely to succeed.“*

In diesem Dokument wird folgende informelle Definition verwendet:

„Ein APT liegt dann vor,
wenn ein typischerweise staatlich gesteuerter Angreifer zum Zweck der Spionage oder Sabotage
über einen längeren Zeitraum hinweg sehr gezielt ein Netz oder System angreift,
sich unter Umständen darin bewegt und/oder ausbreitet
und so Informationen sammelt oder Manipulationen vornimmt.“

Damit unterscheiden sich APTs deutlich von der Masse der Angriffe, denn im Regelfall wollen die Angreifenden mit möglichst geringem Aufwand einen größtmöglichen, meist finanziellen Gewinn erzielen. Sollten sie dabei auf Hindernisse stoßen, die nicht mit einfachen Mitteln zu umgehen sind, ziehen sie zum

nächsten, einfacher verwundbaren Opfer weiter. Daher ist ein wesentlicher Aspekt der hier zugrundeliegenden Definition für APTs die langfristige Ausrichtung des Angriffs, d.h. dass der Angreifer nicht aufgibt, bis ihm ein Zugriff und u.U. auch ein Festsetzen in den Netzen gelungen ist. Um dabei keine Aufmerksamkeit zu erregen und eine Entdeckung zu vermeiden bzw. möglichst lange hinaus zu zögern, bereitet er sich umfassend vor und agiert anschließend sehr systematisch und vorsichtig. Selbst wenn der Angriff entdeckt und ggf. auch erfolgreich abgewehrt wird, ist die Wahrscheinlichkeit dennoch sehr groß, dass die Angreifenden zu einem späteren Zeitpunkt (ggf. über einen anderen Einfallsvektor) wiederkehren.

Weitergehende Information zum Vorgehen der Täter (sowie zur sogenannten Kill Chain) können Sie den APT-Präventions-Dokumenten entnehmen:

TLP:GREEN **Advanced Persistent Threats – Teil 1 Prävention**
Rechtliche und strategische Maßnahmen für das Management
Managementhinweise zur rechtlichen Verantwortung, Einbindung relevanter Stellen und zu strategischen Entscheidungen, BSI 2021

TLP:AMBER **Advanced Persistent Threats – Teil 2 Prävention**
Technische und organisatorische Maßnahmen für die Vorfallsbearbeitung
Anlassbezogene und akute Hilfestellungen, BSI 2021

Detektionsmöglichkeiten entlang der Kill Chain werden im APT-Detektions-Dokument beschrieben:

TLP:AMBER **Advanced Persistent Threats – Teil 3 Detektion**
Technische und organisatorische Maßnahmen für die Vorfallsbearbeitung
Anlassbezogene und akute Hilfestellungen, BSI 2021

3 Literaturverzeichnis

BSI2019a Bundesamt für Sicherheit in der Informationstechnik, *IT-Grundschutz-Kompendium: Werkzeug für Informationssicherheit*, https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/it-grundschutz-kompendium_node.html, Aufgerufen am 15.02.2021

Sch2011 Bruce Schneier, 2011, *Advanced Persistent Threat (APT)*, https://www.schneier.com/blog/archives/2011/11/advanced_persis.html, Aufgerufen am 06.05.2020

TLP:WHITE

Bundesamt
für Sicherheit in der
Informationstechnik

Modul 1: Incident Response

1 Vorbemerkungen

ⓘ In diesem Modul erfahren Sie:

- ☑ In welche Phasen ein typischer Incident Response Prozess unterteilt ist.
- ☑ Woran Sie erkennen, ob es sich bei dem detektierten Angriff um einen APT-Angriff handelt.
- ☑ Was Sie bei einem APT-Angriff unternehmen sollten.
- ☑ Welche weiteren Maßnahmen Sie während der jeweiligen Phasen erwägen/ergreifen sollten.

Wichtige Hinweise

Anspruch und Ziel des vorliegenden Moduls ist eine erste Information/Hilfestellung zum Thema „Incident Response“ zu geben. Das Modul kann dabei nicht auf unternehmensspezifische Besonderheiten eingehen.

Wichtiger Hinweis

Die hier angebotene Fassung des Dokuments beinhaltet lediglich Auszüge, da die Inhalte dieses Moduls TLP:AMBER eingestuft sind. Das vollständige Dokument erhalten Sie im passwortgeschützten INSI-Bereich der Allianz für Cybersicherheit sowie im Falle der Vorfallsbearbeitung von CERT-Bund.

TLP:WHITE

Bundesamt
für Sicherheit in der
Informationstechnik

Modul 2: Incident Management

1 Vorbemerkungen

ⓘ In diesem Modul erfahren Sie:

- ☑ Wie Sie (auch ohne Vorerfahrung) am besten mit dem Incident Management beginnen.
- ☑ Warum Information Sharing bei APTs elementar wichtig ist.
- ☑ Welche externen Experten Sie hinzuziehen können / sollten und wie Sie sich am besten auf die Zusammenarbeit vorbereiten.

Inhalt

1 Vorbemerkungen 11
2 Ruhiges und besonnenes Vorgehen 12
3 Incident Handling als Projekt 13
4 Der APT-Angriff als Teil einer Kampagne 15
4.1 Information Sharing 15
5 Externe Unterstützung 16
5.1 Bundesamt für Sicherheit in der Informationstechnik (BSI) 16
5.2 Landes- bzw. Bundesamt für Verfassungsschutz 17
5.3 Polizeien 17
5.4 Sicherheitsdienstleister 18
5.5 Vorbereitungen für die externe Unterstützung 18
5.6 Übersicht – Externe Unterstützung 19
6 Glossar 20
7 Abkürzungsverzeichnis 21
8 Literaturverzeichnis 22
Modul 2 – Anhang A Vorbereitungen für die externe Unterstützung 23

2 Ruhiges und besonnenes Vorgehen

Aus der Erfahrung des Bundesamts für Sicherheit in der Informationstechnik (BSI) haben Angreifende die Systeme eines Betroffenen meist bereits seit Wochen oder Monaten unter ihrer Kontrolle bevor der Angriff entdeckt wird. IT-Sicherheitsdienstleister und -forscher kommen in ihren Fallstudien zu ähnlichen Ergebnissen: Demnach dauerte es in den letzten Jahren im Schnitt zwischen 100 und 200 Tagen, bis ein APT-Angriff entdeckt wurde (vgl. z. B. [Pon2018], [Fir2018], [Mic2016]). Selbst wenn ein Angriff relativ früh entdeckt wird, ist die Wahrscheinlichkeit groß, dass **die Daten**, an denen der Angreifende interessiert ist und auf welche er Zugriff hat, **bereits abgeflossen** sind. **Daher wird zusätzliche Zeit, welche für die Planung des Vorgehens, für die Analyse und für die Bereinigung investiert wird, die Auswirkungen des Vorfalls in der Regel nicht verschlimmern.** Stattdessen ist eine Analyse des Ausmaßes der Kompromittierung und eine sorgfältige Vorbereitung der Bereinigung notwendig.

Schnellschüsse (die leider in der Praxis noch immer oft vorkommen) wie nur ein einzelnes auffällig gewordenes infiziertes System zu bereinigen, könnten den Angreifenden alarmieren und zu weiteren maliziösen / gefährlichen Maßnahmen veranlassen. Er könnte in der Folge weitere Hintertüren einbauen, kurzfristig möglichst viele Daten stehlen, Spuren auf anderen Systemen, die noch unter seiner Kontrolle sind, vernichten oder im schlimmsten Fall sogar Sabotage-Aktivitäten an den Daten und Netzen durchführen.

Daher sollten Sie davon ausgehen, dass die Angreifenden zu dem Zeitpunkt ihrer Entdeckung wahrscheinlich bereits das gesamte Netzwerk aufgeklärt haben und vermutlich über einen besseren und aktuelleren Netzplan als Ihre eigenen Administratoren verfügen. In manchen Fällen etablieren die Angreifenden im Netzwerk zudem sogenannte Brückenköpfe, welche als einzige aktiv mit der Außenwelt (z.B. zu einem Command and Control (C&C) -Server) kommunizieren. Andere kompromittierte Systeme im Netzwerk kommunizieren wiederum nur mit den Brückenköpfen. Wird jetzt auf die Schnelle nur ein Brückenkopf bereinigt, weil nur dieser in den ersten Analysen aufgefallen ist, kann der Angreifende über bereits vorher angelegte zusätzliche Hintertüren auf den anderen Systemen die Kontrolle über Ihr Netzwerk zurückerlangen.

In jedem Fall sollte das Management frühzeitig informiert und diesem insbesondere die Dimension und die Konsequenzen eines solchen Angriffs aufgezeigt werden. Insbesondere etwaige Risikoabschätzungen, die im Zuge des Incident Response Prozesses (siehe Modul 1) getroffen werden müssen, basieren nicht auf einer rein fachlichen IT-Bewertung, sondern bedürfen einer organisationsweiten Risikobewertung. Daher sind die Bewertung und schließlich auch die Genehmigung eines Vorgehens auf der obersten Führungsebene der Organisation zu treffen.

Weitergehende Informationen für das Management zum Themengebiet „Reaktion“ finden Sie auch in der folgenden Publikation:

TLP:GREEN Advanced Persistent Threats – Teil 5 Reaktion
Strategische Maßnahmen zur Reaktion für das Management
Wo zieht man im Angriffsfall rote Linien?, BSI 2021

3 Incident Handling als Projekt

Die wenigsten Unternehmen haben bereits Erfahrung mit der Bewältigung größerer IT-Sicherheitsvorfälle. Daher existieren oft auch keine vorbereiteten Pläne und Strukturen, wenn ein APT-Angriff festgestellt wird.

Wichtiger Hinweis

Es ist an dieser Stelle nochmal zu betonen, dass APTs nicht durch einzelne Maßnahmen verhindert werden können (bzw. generell sehr schwer zu verhindern sind, da nie ausgeschlossen werden kann, dass die Angreifenden über bisher unbekannte Zero Days oder andere neue Angriffstechniken verfügen), sondern dass das Sicherheitsniveau durch die Summe der umgesetzten Maßnahmen bestimmt wird. Dabei spielen auch solche Maßnahmen eine Rolle, die nicht explizit auf APTs abzielen, sondern die die Basis-Sicherheit erhöhen (z.B. Netzwerk-Firewall, Anti-Viren-Schutz, Schnittstellenkontrolle und Patch-Management).

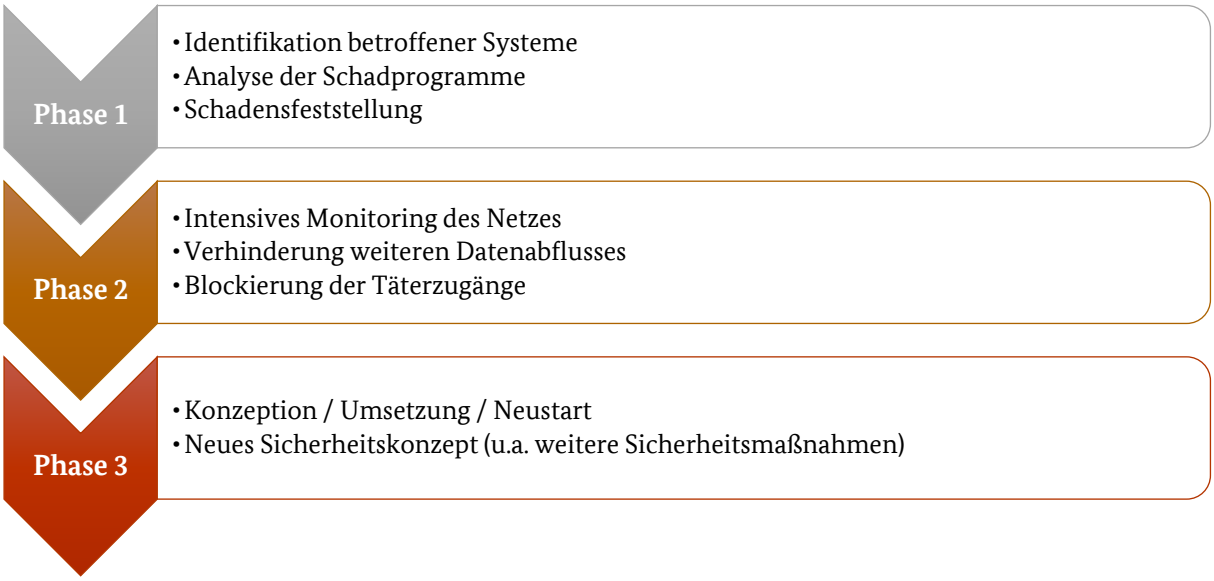
Daher gilt es auch bei der Abwehr von APTs die bereits bekannten Basismaßnahmen zur IT-Sicherheit (wie das IT-Grundschutz-Kompendium des BSI, vgl. [BSI2020], Basismaßnahmen der Cyber-Sicherheit [BSI2018c] und relevante Mindeststandards, vgl. z.B. [BSI2018a]) umzusetzen.

Weitergehende Informationen zum Themengebiet Prävention finden Sie auch in den folgenden Publikationen:

TLP:GREEN **Advanced Persistent Threats – Teil 1 Prävention**
Rechtliche und strategische Maßnahmen für das Management
Managementhinweise zur rechtlichen Verantwortung, Einbindung relevanter Stellen und zu strategischen Entscheidungen, BSI 2021

TLP:AMBER **Advanced Persistent Threats – Teil 2 Prävention**
Technische und organisatorische Maßnahmen für die Vorfallsbearbeitung
Anlassbezogene und akute Hilfestellungen, BSI 2021

Die meisten betroffenen Firmen/Institutionen haben aber bereits Erfahrungen mit der Durchführung von größeren Projekten gemacht. Deshalb kann es sinnvoll sein, bei fehlender Vorbereitung, das Incident Handling im Notfall als Projekt anzusehen und dieses auch mit den Mitteln des Projektmanagements anzugehen. Dafür kann man den Ablauf wie folgt grob in drei Phasen unterteilen:



Wichtiger Hinweis

Auch an dieser Stelle sei noch einmal darauf hingewiesen, dass Erfahrungen mit der Bewältigung von größeren APT-Angriffen zeigen, dass man für die einzelnen Phasen eher mit Wochen und Monaten als mit Tagen kalkulieren muss (siehe auch Modul 1).

4 Der APT-Angriff als Teil einer Kampagne

In der Regel ist ein APT-Angriff auf eine Institution / Unternehmen kein isoliertes Ereignis. Eine Angriffsserie richtet sich meistens gegen eine ganze Gruppe von Institutionen / Unternehmen, wie zum Beispiel:

- Unternehmen, die alle im gleichen Sektor tätig sind (vor allem Rüstungsindustrie, Hochtechnologiebranchen, Forschungseinrichtungen und öffentliche Verwaltung).
- Unternehmen, die alle eine bestimmte Technologie einsetzen.
- Unternehmen, die alle denselben Kunden (z.B. im Verteidigungsbereich) haben.
- Unternehmen, die alle denselben Zulieferer haben (Supply Chain Angriffe).

Zusammengefasst nennt man eine solche Serie von Angriffen eine APT-Kampagne. Dabei ist zu beobachten, dass die Angreifenden oftmals dieselbe Infrastruktur für unterschiedliche Angriffe wiederverwenden. Das können dann z.B. dieselben C&C-Server oder auch dieselbe Schadsoftware sein.

4.1 Information Sharing

Für einen einzelnen Betroffenen einer solchen APT-Kampagne kann es sehr schwierig sein, frühzeitig Anzeichen für eine erfolgreiche Kompromittierung zu entdecken. Abhilfe kann aber dadurch geschaffen werden, dass Institutionen/Unternehmen, die einen APT-Angriff bei sich entdecken diesen an eine kompetente Stelle (z.B. das BSI) melden, damit diese dann in geeigneter Form weitere mögliche Betroffene informieren kann. Dabei sollten Sie unbedingt Ihre Bereitschaft dafür erklären, dass Angriffs-Informationen mit anderen Unternehmen und Sicherheitsteams ausgetauscht werden dürfen – dies geschieht natürlich immer in so einer anonymisierten Form, dass es dabei keinen Hinweis auf Sie selbst gibt!

Wichtiger Hinweis

Wer selber nicht vernetzt ist und aktiv beiträgt, wird oftmals auch nicht unterrichtet, wenn ein Anderer wertvolle Informationen besitzt. Bedenken Sie also, dass auch Sie selbst hilfreiche Informationen über ähnliche Angriffe erhalten können, die dann die Bewältigung eines Vorfalls erheblich erleichtern und beschleunigen!

Zudem ist es wichtig, dass auch versuchte (d.h. nicht erfolgreiche) Angriffe an eine kompetente zentrale Stelle, wie das BSI, gemeldet werden. Auch wenn Sie den APT-Angriff erfolgreich abwehren konnten, könnte der gleiche Angriff bei einem Ihrer Kunden, Partner oder Zulieferer erfolgreich verlaufen sein. Auch hier sollten Sie Informationen über den Angreifenden sowie seine Technik und Methoden (sogenannte „Tactics, Techniques, and Procedures“ (TTP)) weitergeben. Für Sie selbst handelt es sich natürlich um einen herausgehobenen Einzelfall – für die Helfer ist es jedoch nur einer von vielen Fällen (aus diesen kumulierten Informationen lassen sich dann wiederum weitere Informationen und Handlungsempfehlungen ableiten).

Eine sehr einfache Möglichkeit, einen Angriff(sversuch) an das BSI zu melden, bietet z.B. das Online-Meldeformular der Allianz für Cyber-Sicherheit (ACS)[1]. Weitere Informationen zur Zusammenarbeit mit dem BSI und anderen relevanten Helfern/Playern finden Sie auch im folgenden Abschnitt.

[1] Meldeformular der ACS:
https://www.allianz-fuer-cybersicherheit.de/Webs/ACS/DE/IT-Sicherheitsvorfall/Unternehmen/Online-Meldung/online-meldung_node.html

5 Externe Unterstützung

Oftmals besitzen selbst große Firmen nicht genug interne Expertise für erfolgreiches Incident Handling bei einem APT-Angriff. **Für viele Unternehmen ist es sogar das erste Mal, dass sie überhaupt mit dem Begriff „APT" konfrontiert werden. Ziehen Sie daher frühzeitig externe Experten hinzu, die Sie kompetent unterstützen können.**

Zudem sollten Sie auch die Möglichkeit in Betracht ziehen, dass Ihr Unternehmen gar nicht das finale Ziel der Angreifenden ist/war, sondern lediglich als Ausgangspunkt/Sprungbrett für weitere Angriffe dient/diente. Das bedeutet, dass möglicherweise auch die Systeme von Kunden, Zulieferern oder Partnern durch die Interaktion mit Ihrem Netzwerk kompromittiert werden können/wurden (eine besondere Form im Bereich der Software-Entwicklung spielen dabei sogenannte **Supply-Chain-Angriffe**). Incident Handling, das sich nur auf das eigene Unternehmen (bzw. auf die Unternehmensnetzwerke) beschränkt, wäre dann nicht ausreichend.

Folgende Hinweise bezüglich externer Unterstützung gelten für Unternehmen innerhalb Deutschlands. In anderen Ländern müssen die entsprechenden lokalen Behörden kontaktiert werden.

5.1 Bundesamt für Sicherheit in der Informationstechnik (BSI)

Das BSI ist ein kompetenter Ansprechpartner im Fall eines APT-Angriffs, da es über fundierte Kenntnisse und viel Erfahrung bei der Behandlung von APT-Angriffen verfügt. Insbesondere bei den folgenden Punkten kann Sie das BSI unterstützen:

- Besprechung von Maßnahmen (Telefonkonferenz, Videotelefonie, E-Mail, Vor-Ort-Besuche, usw.)
- Unterstützung durch vorbereitete Dokumente mit Empfehlungen und Vorgehensweisen
- Vermittlung von (Forensik-)Experten (mit Hilfe eines aufwendigen Prüfverfahrens hat das BSI geeignete Sicherheitsdienstleister als APT-Response Dienstleister qualifiziert[2])
- Koordination des Informationsaustausches mit anderen Experten oder Betroffenen, z.B. über Angriffssignaturen sog. Indicators of Compromise (IoC)
- Unterstützung bei der Kontaktaufnahme mit dem entsprechenden Landes- oder Bundesamt für Verfassungsschutz
- Unterstützung bei der Kontaktaufnahme mit den Strafverfolgungsbehörden

Detaillierte Informationen zum Unterstützungsangebot des BSI können sie auch der folgenden BSI-Publikation entnehmen:

Vorfallsunterstützung für die Bundesverwaltung, Kritische Infrastrukturen und bei herausgehobenen Fällen, Bundesamt für Sicherheit in der Informationstechnik, 2018

Wie bereits vorher beschrieben, werden bei APT-Angriffen oftmals dieselbe Infrastruktur und / oder dieselbe Schadsoftware genutzt, um mehrere Unternehmen im Zuge einer Kampagne anzugreifen. Hier kann das BSI durch die Verknüpfung mit anderen Fällen Zusammenhänge herstellen und Hinweise aus diesen Fällen, wie IoCs, mit anderen (potentiell) Betroffenen teilen, ohne dass dabei die Identitäten der einzelnen Betroffenen bekannt werden.

Die Zusammenarbeit mit dem BSI erfolgt stets streng vertraulich. Das BSI wird – ohne Ihre explizite Zustimmung – keine Sie identifizierenden Informationen zu dem Vorfall an Dritte weitergeben.

[2] Die Liste der qualifizierten APT-Response Dienstleister finden Sie hier: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Dienstleister_APT-Response-Liste.html

Zur Kontaktaufnahme verwenden Sie entweder das Online-Formular der Allianz für Cybersicherheit[3] oder Sie wenden sich direkt an das Computer Emergency Response Team (CERT-Bund)[4].

5.2 Landes- bzw. Bundesamt für Verfassungsschutz

Bei einem Verdacht auf Wirtschaftsspionage, sollten Sie sich an das für Sie zuständige Landesamt für Verfassungsschutz (LfV) wenden. Auch die Zusammenarbeit mit dem LfV erfolgt stets streng vertraulich. Ebenfalls liegen dem LfV häufig Erkenntnisse aus anderen, ähnlich gelagerten, Fällen vor, die bei einer Meldung herangezogen werden können. Dadurch kann das LfV Zusammenhänge zwischen Vorfällen herstellen und hilfreiche Schlüsse ziehen.

Für präventiven Wirtschaftsschutz ist aber auch das Bundesamt für Verfassungsschutz (BfV) zuständig. Im Rahmen der **„Initiative Wirtschaftsschutz“**[5] haben sich deshalb die vier deutschen Sicherheitsbehörden BfV, Bundeskriminalamt (BKA), Bundesnachrichtendienst (BND) und BSI zusammengeschlossen, um Unternehmen gebündelt ihre Expertise zur Verfügung zu stellen. Dort finden Sie auch alle wichtigen Erreichbarkeiten bei den Landesämtern für Verfassungsschutz und beim Bundesamt für Verfassungsschutz[6].

5.3 Polizeien

Bei einem APT-Angriff werden von den Angreifenden in der Regel mehrere Straftaten begangen, insbesondere solche nach §§ 202a, 202b, 202c, 303a und 303b Strafgesetzbuch (StGB). Dazu zählen das Ausspähen und Abfangen von Daten bzw. entsprechende Vorbereitungen sowie die Veränderung von Daten und Computersabotage. **Das BSI empfiehlt daher grundsätzlich bei einem APT-Angriff Strafanzeige bei der für Sie zuständigen Polizei zu stellen**.

Wie bereits in Modul 1 beschrieben, können die Strafverfolgungsbehörden zudem je nach Vorfall z.B. weitere Informationen erlangen, Server sicherstellen oder Angriffe zurückverfolgen.

Das Bundeskriminalamt bzw. die zuständigen Landeskriminalämter haben für diese Zwecke Anlaufstellen eingerichtet (Zentralen Ansprechstellen Cybercrime für die Wirtschaft (ZAC)), die Opfern von Cyber-Straftaten beratend zur Seite stehen und bei einer Anzeige unterstützen. Eine Liste der Anlaufstellen, sowie vielfältige weitere Informationen zum Thema finden Sie auf den Webseiten des Bundeskriminalamts[7], der Allianz für Cybersicherheit[8] oder auf den Webseiten der „Initiative Wirtschaftsschutz“[9].

Beachten Sie, dass bei einer Anzeige mögliche Beweise gerichtsfest erhoben und alle Vorgänge entsprechend dokumentiert werden müssen.

[3] Meldeformular der ACS: https://www.allianz-fuer-cybersicherheit.de/Webs/ACS/DE/IT-Sicherheitsvorfall/Unternehmen/Online-Meldung/online-meldung_node.html
[4] CERT-Bund: https://www.bsi.bund.de/CERT-Bund
[5] Initiative Wirtschaftsschutz: https://www.wirtschaftsschutz.info
[6] Zuständigkeit Verfassungsschutzbehörden: https://www.wirtschaftsschutz.info/DE/Ansprechpartner/Verfassungsschutz/verfassungsschutz_node.html
[7] Zuständigkeit Polizeien: https://www.polizei.de/Polizei/DE/Einrichtungen/ZAC/zac_node.html
[8] Zuständigkeit Polizeien (ACS): https://www.allianz-fuer-cybersicherheit.de/Webs/ACS/DE/IT-Sicherheitsvorfall/Unternehmen/Kontakt-zur-Polizei/Zentrale-Ansprechstellen-Cybercrime/zentrale-ansprechstellen-cybercrime_node.html
[9] Zuständigkeit Polizeien (Initiative Wirtschaftsschutz): https://www.wirtschaftsschutz.info/DE/Themen/Cybercrime/Ansprechpartner/ZACErreichbarkeiten.html?nn=7474096

5.4 Sicherheitsdienstleister

Externe Sicherheitsdienstleister können Sie professionell und personell bei der Vorfallsbearbeitung unterstützen. Allgemein ist bei der Auswahl eines Sicherheitsdienstleisters zu beachten, dass die Unternehmen häufig unterschiedliche Analyseschwerpunkte haben. Die Bandbreite des Knowhows reicht dabei von der Analyse netzwerkbasierter APT-Angriffen bis hin zur Wiederherstellung von physisch zerstörten Festplatten.

Ein geeigneter APT-Response Dienstleister sollte bereits Erfahrungen in diesem Umfeld und Kenntnisse in den Bereichen Festplatten-, Speicher-, Netzwerkforensik sowie Logdatenerfassung und Auswertung haben. Daneben sind Betriebssystem-Experten, insbesondere Active Directory Logauswertungsexperten, oftmals sehr hilfreich.

Wie bereits beschrieben, hat das BSI im Rahmen eines umfangreichen Auswahlverfahrens mehrere Sicherheitsdienstleister als APT-Response Dienstleister qualifiziert[10].

5.5 Vorbereitungen für die externe Unterstützung

Damit die externen Experten im Ernstfall schnell mit der Bearbeitung des Vorfalls beginnen zu können (und nicht wertvolle Zeit mit Vorbereitungen verlieren), können und sollten Sie Ihrerseits bereits einige vorbereitende und unterstützende Maßnahmen treffen. Eine umfangreiche Checkliste für diese Vorbereitung finden Sie in Anhang A dieses Moduls.

[10] Die Liste der qualifizierten APT-Response Dienstleister finden Sie hier:
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Dienstleister_APT-Response-Liste.html

5.6 Übersicht – Externe Unterstützung

Externer Experte	*Information*	*Link*
BSI	Meldeformular ACS	https://www.allianz-fuer-cybersicherheit.de/Webs/ACS/DE/IT-Sicherheitsvorfall/Unternehmen/Online-Meldung/online-meldung_node.html
	CERT-Bund	https://www.bsi.bund.de/CERT-Bund
Landes- bzw. Bundesamt für Verfassungsschutz	Liste der Erreichbarkeiten	https://www.wirtschaftsschutz.info/DE/Ansprechpartner/Verfassungsschutz/verfassungsschutz_node.html
Polizeien	Liste der Erreichbarkeiten	https://www.polizei.de/Polizei/DE/Einrichtungen/ZAC/zac_node.html
APT-Response Dienstleister	Qualifizierte APT-Response Dienstleister	https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Dienstleister_APT-Response-Liste.html
Initiative Wirtschaftsschutz	Kooperation von BfV, BKA, BND und BSI	https://www.wirtschaftsschutz.info
Allianz für Cyber-Sicherheit	Initiative von BSI und bitkom	https://www.allianz-fuer-cybersicherheit.de/

6 Glossar

Supply-Chain-Angriff Supply-Chain-Angriffe zielen vor allem auf Softwareentwickler und Lieferanten ab und basieren darauf, dass legitime Anwendungen häufig Software-Bibliotheken von Drittanbietern nutzen. Die Angreifenden kompromittieren dafür das Netzwerk eines Softwareentwicklers/Lieferanten und fügen Schadcode in dessen Software (Quellcode) ein. Verwendet nun ein anderes Unternehmen diese Software-Bibliothek für seine Anwendung, wird auch der Schadcode (zum Beispiel beim nächsten Update) weiterverbreitet. So erreichen es die Angreifenden, dass ihr Schadcode über eigentlich legitime Anwendungen verteilt wird.

7 Abkürzungsverzeichnis

ACS	Allianz für Cyber-Sicherheit
BfV	Bundesamt für Verfassungsschutz
BKA	Bundeskriminalamt
BND	Bundesnachrichtendienst
BSI	Bundesamt für Sicherheit in der Informationstechnik
C&C	Command and Control
CERT	Computer Emergency Response Team
IoC	Indicator of Compromise
LfV	Landesamt für Verfassungsschutz
StGB	Strafgesetzbuch
TTP	Tactics, Techniques, and Procedures
ZAC	Zentrale Ansprechstelle Cybercrime

8 Literaturverzeichnis

BSI2018a Bundesamt für Sicherheit in der Informationstechnik, 2018, *Mindeststandard des BSI zur Protokollierung und Detektion von Cyber-Angriffen*, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindeststandard_BSI_Protokollierung_und_Detektion_Version_1_0.pdf?__blob=publicationFile&v=4, Aufgerufen am 02.04.2019

BSI2018c Bundesamt für Sicherheit in der Informationstechnik, 2018, *Basismaßnahmen der Cyber-Sicherheit*, https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_006.pdf?__blob=publicationFile&v=1, Aufgerufen am 16.02.2021

BSI2020 Bundesamt für Sicherheit in der Informationstechnik, 2020, *IT-Grundschutz-Kompendium – Werkzeug für Informationssicherheit*, https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/it-grundschutz-kompendium_node.html, Aufgerufen am 15.02.2021

Fir2018 FireEye, Inc., 2018, *Mandiant M-TRENDS 2018*, FireEye, Inc., 2018

Mic2016 Microsoft Corporation, 2016, *Microsoft Advanced Threat Analytics*, Microsoft Corporation, 2016

Pon2018 Ponemon Institute LLC, 2018, *Cost of a Data Breach Study: Global Overview*, Ponemon Institute LLC, 2018

TLP:WHITE

Bundesamt
für Sicherheit in der
Informationstechnik

Modul 2 - Anhang A

Vorbereitungen für die externe Unterstützung

Logistik		
1	Ggf. Bereitstellung von Zimmern in einem gemeinsamen angemessenen Hotel für das ganze Team mit Frühstück. Das Hotel sollte in der Nähe (am besten fußläufig) des Einsatzortes liegen. Alternativ: Benennung eines geeigneten Hotels in räumlicher Nähe zum Einsatzort	☐
2	Ggf. geeigneter Unternehmens-Hotel-Shuttle bei entfernteren Hotels (nach Absprache)	☐
3	Verpflegung während der Arbeitszeit vor Ort	☐
4	Softdrinks und Wasser vor Ort	☐
5	Team bei der Pforte / Wachschutz anmelden	☐
6	Vorab dem Team etwaige Besonderheiten am Einsatzort mitteilen (z.B. Rauchverbot im Werk, Sicherheitsvorschriften, etc.)	☐

Räume		
1	Arbeitsraum für mind. 4-8 Mitarbeiter/innen mit freier Wand für Beamer-Anzeige (Möglichst in räumlicher Nähe zu den Incident Handlern bzw. relevanten IT-Betriebskomponenten Ihres Unternehmens)	☐
2	Nach Möglichkeit mit Klimatisierung, da die zahlreiche eingesetzte IT den Raum zusätzlich erwärmt	☐
3	Nach Möglichkeit mit mindestens 2x 16A Stromkreisläufen für die zahlreiche Technik	☐
4	Falls möglich 2. Raum (Besprechungsraum) für Meetings, Video/Telefon-Konferenzen, um die arbeitenden Kollegen nicht zu stören	☐

IT-Infrastruktur		
1	Freier Breitband Internet-Zugang (über ein nicht kompromittiertes Netz), für VPN freigeschaltet.	☐
2	Anschluss ans interne Netz (wenn möglich)	☐
3	Zugriff auf zentral abgelegte Logs von Tools	☐

Informationen

Hinweis: Um bestmögliche Unterstützung leisten zu können ist es für das Vor-Ort-Team erforderlich, sich in kürzester Zeit in die Besonderheiten Ihrer Institution / Ihres Unternehmens einzuarbeiten. Die notwendigen Informationen gliedern sich dabei in allgemeine Informationen zum Unternehmen, in technische Informationen sowie Informationen zum Vorfall auf. Diese Informationen sollten Sie im Rahmen einer Einsatz-Einführungsveranstaltung nach Eintreffen des Vor-Ort-Teams vorstellen.

Allgemeine Informationen		
1	Standorte, Geschäftspartner, Zulieferer, Marken-Philosophie, Kronjuwelen (besonders schützenswerte wettbewerbsrelevante Informationen und Prozesse), kritische Geschäftsprozesse und Anlagen für die Erbringung der Dienstleistung, Betriebsvereinbarung, usw.	☐
2	Wie ist die private Nutzung des Internets geregelt? Dürfen Sie auf die Log-Daten zugreifen und forensisch mit MA-PCs arbeiten?	☐
3	Ist der Personalrat bereits informiert? Gibt es hier einen Plan? Hat er den Einsatz freigegeben? Ist ein erläuterndes Hintergrundgespräch des externen Experten zur Bedrohungslage und den notwendigen Analysen und Maßnahmen mit dem Personalrat gewünscht?	☐
4	Ist der Datenschutz bereits informiert? Gibt es hier einen Plan? Hat er den Einsatz freigegeben? Ist ein erläuterndes Hintergrundgespräch des externen Experten zur Bedrohungslage und den notwendigen Analysen und Maßnahmen mit dem Datenschutz gewünscht?	☐
5	Ist die Pressestelle bereits informiert? Gibt es hier einen Kommunikationsplan? Ist ein erläuterndes Hintergrundgespräch des externen Experten zur Bedrohungslage und den notwendigen Analysen und Maßnahmen mit der Pressestelle gewünscht?	☐
6	Sind die Partner-/ Kunden- und Zuliefererbetreuer bereits informiert? Gibt es hier einen Kommunikationsplan? Ist ein erläuterndes Hintergrundgespräch zur Bedrohungslage und den notwendigen Analysen und Maßnahmen des externen Experten mit den Kunden- und Zuliefererbetreuern gewünscht?	☐

Technische Informationen		
1	Netzplan *Hinweis: Es reicht einen Übersichtsplan zu übergeben. Für die Details muss ein auskunftsfähiger Ansprechpartner benannt werden, auf den kurzfristig zugegriffen werden kann und der bei der Auswertung und Analyse unterstützt*	☐
2	Sicherheitsmaßnahmen (Passwort Policy, Sicherheitsmaßnahmen für Admin-Zugriffe, Logging und Orte des Loggings)	☐

Informationen zum Vorfall		
1	Was ist passiert: Was ist das Problem? Wie äußert es sich? Seit wann besteht das Problem? Was könnte die Ursache sein? Was heißt das für Ihr Unternehmen und für Ihre Kunden/Partner/Zulieferer als mögliche weitere Betroffene?	☐
2	Ergriffene Maßnahmen: Wer in Ihrem Unternehmen arbeitet daran? Was wurde bereits unternommen? Was hat funktioniert? Was nicht? Warum?	☐
3	Erwartungsmanagement: Wie können die externen Experten helfen? Was brauchen Sie? Was erwarten Sie sich?	☐

Informationen zu weiteren beteiligten Parteien		
1	Wurde ein Beratungsunternehmen zur Behandlung des Vorfalls beauftragt? Wer? *Hinweis: Sollten Sie zusätzlich mit dem BSI zusammenarbeiten, geben Sie bitte dem Unternehmen die Freigabe, mit dem BSI über den Sachverhalt zu sprechen und Daten auszutauschen!*	☐
2	Wurde Anzeige erstattet? Bei wem? Aktenzeichen, Ansprechpartner? Ist das LKA / Zentrale Ansprechstelle Cyber-Crime (ZAC) eingebunden? *Hinweis: Das BSI hat über das Cyber-Abwehrzentrum Kontakte zum BKA und damit Richtung Polizeien. Gerade bei konkreten C2 Servern in DE kann dort hilfreich unterstützt werden. Ist es gewünscht, dass das BSI hier vermittelt?*	☐
3	Falls ein nachrichtendienstlicher Hintergrund besteht, gibt es eine gesetzliche Zuständigkeit des Bundesamtes für Verfassungsschutz (BfV). Wurden diese eingebunden? *Hinweis: Das BSI muss das BfV über nachrichtendienstliche Fälle unterrichten. Sie können einer Weitergabe Ihres Unternehmensnamens durch das BSI widersprechen (Bitte eine kurze schriftliche Notiz.) Bedenken Sie, dass das BfV weiterführende Informationen zum Angreifenden haben könnte, sodass eine geeignete Einbindung geprüft werden sollte.*	☐

Daten

Hinweis: Welche Logs sinnvollerweise zur Verfügung gestellt werden sollten, sollte im Einzelfall vorab besprochen werden. Viele Hinweise auf wertvolle Logdaten sowie Anleitungen, wie Sie diese sammeln können, finden Sie in Modul 3.

Daten		
1	Abklärung, welche Logdaten der externe Experte vor Ort analysieren muss und welche er in das eigene Labor mitnehmen darf	☐

Ansprechpartner/innen		
1	Ansprechpartner/innen benennen und die externe Unterstützung ankündigen bzw. die Mitarbeiter/innen persönlich vorstellen. Dazu gehören auch Ansprechpartner/innen bei IT-Dienstleistern für relevante Systeme.	☐
2	Liste der Ansprechpersonen erstellen (Name, Telefonnummer, Mailadresse). Je nach Umfang / Bedarf in Ihrem Unternehmen die Kontakte zu: • CIO/CISO • Abteilungsleiter/in IT-Sicherheit • Referatsleiter/in IT-Sicherheit • Referatsleiter/in IT-Betrieb • Interne Incident Handler • IT-Sicherheitsbeauftrage/r • Datenschutzbeauftragte/r • Personalvertreter/in • Rechtsberater/Juristen • Netz-Administrator • Firewall-Administrator • AD/DC-Administrator • Krisenmanager/in • Pressesprecher/in bzw. Ansprechperson für interne Kommunikation	☐

TLP:WHITE

Bundesamt
für Sicherheit in der
Informationstechnik

Modul 3: Technische Analyse

1 Vorbemerkungen

ⓘ In diesem Modul erfahren Sie:

- ☑ Wie Sie die für die forensische Analyse benötigten Daten sammeln.
- ☑ Was der Unterschied zwischen Live Response und Post Mortem Analyse ist.
- ☑ Wie Sie ein forensisches Datenträgerabbild mit CAINE erstellen.
- ☑ Wie Sie mit Ihrer Antiviren-Software im APT-Fall umgehen sollten.
- ☑ Wie Sie mit Logdaten umgehen sollten.
- ☑ Wie und wo Sie Netzwerkverkehr in Ihren Systemen aufzeichnen sollten.
- ☑ Welche weiteren potentiell interessanten Artefakte es gibt.
- ☑ Wie Sie am besten mit der Analyse der gesammelten Daten beginnen.

Wichtige Hinweise

Anspruch und Ziel des vorliegenden Moduls ist eine erste Information/Hilfestellung zum Thema „Technische Analyse bei APT-Angriffen“. Das Modul kann nicht auf unternehmensspezifische Besonderheiten eingehen, es kann keine professionelle forensische Untersuchung und auch keine individuelle Unterstützung durch (externe) Experten ersetzen.

Wichtiger Hinweis

Die hier angebotene Fassung des Dokuments beinhaltet lediglich Auszüge, da die Inhalte dieses Moduls TLP:AMBER eingestuft sind. Das vollständige Dokument erhalten Sie im passwortgeschützten INSI-Bereich der Allianz für Cybersicherheit sowie im Falle der Vorfallsbearbeitung von CERT-Bund.