TLP WHITE //
~~TLP AMBER~~

Nationales IT-Lagezentrum BSI

CERT Bund

Erste Hilfe bei einem APT-Angriff

Arbeitspapier - Version 3.0

22.01.2016

certbund@bsi.bund.de

0 Einstufung

TLP WHITE: Unbegrenzt

Abgesehen von urheberrechtlichen Aspekten dürfen Informationen der Stufe TLP-WHITE ohne Einschränkungen frei weitergegeben werden.

Inhaltsverzeichnis

1 Über dieses Dokument

Dieses Dokument ist die sanitarisierte TLP WHITE Version des TLP AMBER eingestuften „Erste Hilfe bei einem APT-Angriff“-Dokuments.

Die TLP AMBER Version dient als Notfalldokument für IT-Sicherheitsbeauftrage, CISOs und Systemadministratoren für den Fall eines Verdachts auf einen Advanced Persistant Threat (APT) Angriff auf das Netzwerk und die Systeme einer Institution.

Diese TLP White Version soll möglichen Betroffenen einen Überblick über die Inhalte des Dokumentes geben, ohne in vertrauliche Details zu gehen. So können mögliche Betroffene entscheiden, ob Sie das Dokument beim BSI anfordern wollen.

2 Über Advanced Persistent Threats (APT)

APT, zu deutsch „fortgeschrittene, andauernde Bedrohung“, bezeichnet einen zielgerichteten Cyber-Angriff auf sehr stark eingegrenzte Systeme und Netzwerke. Die Angreifer verfügen in der Regel über hohe finanzielle und personelle Ressourcen. APT Angriffe können nur sehr schwer verhindert werden, da sie oft mit großem Aufwand so entworfen wurden, dass die Standard-Schutzmaßnahmen in Unternehmen umgangen werden.
Bei einem APT-Angriff muss zeitnah eine ganze Reihe an Maßnahmen ergriffen werden. Diese dienen einerseits der Begrenzung des Aktionsradius des Angreifers, dürfen aber andererseits den Angreifer nicht zu früh alarmieren, damit dieser keine Spuren verwischen kann und die Aufklärung des Vorfalls dadurch erschwert oder unmöglich wird.

3 Teil 1 – Incident Management

In diesem Kapitel werden generelle Verhaltensregeln für das Incident Management bei einem APT-Angriff vorgestellt.

3.1 Ruhig bleiben und geplant handeln

In den bekannt gewordenen Fällen hatten Angreifer die Systeme des Opfers meist über Wochen bis Monate unter Ihrer Kontrolle, bevor der Angriff entdeckt wurde. Laut einer Studie[1] über APT-Angriffe von Mandiant wurden die Angriffe im Median erst nach 416 Tagen entdeckt!
Nach Erfahrungen von CERT-Bund werden die meisten Angriffe entweder durch Zufall oder aufgrund eines Hinweises eines Externen entdeckt. Selbst wenn ein Angriff relativ früh entdeckt wird, ist die Wahrscheinlichkeit groß, dass **bereits die Daten**, an denen der Angreifer ein Interesse und auf welche er Zugriff hat, **abgeflossen** sind.
Daher sollte etwas zusätzliche Zeit, welche für die Planung des Vorgehens, für die Analyse und für die Bereinigung investiert wird, den Vorfall in der Regel nicht verschlimmern.

1 Mandiant Trend Report - http://www.mandiant.com/resources/m-trends/

Im Vordergrund sollte die geordnete Analyse des Ausmaßes des Angriffs stehen. Erst wenn alle wichtigen Informationen gesichert sind, sollte eine geplante Bereinigung des eigenen Netzwerkes durchgeführt werden.
Schnellschüsse, die leider in der Praxis oft vorkommen, wie nur ein einzelnes infiziertes System zu bereinigen, könnten den Angreifer alarmieren und zu weiteren Maßnahmen veranlassen. Dieser könnte in der Folgen Spuren auf anderen Systemen, die noch unter seiner Kontrolle sind, vernichten oder im schlimmsten Fall sogar Sabotage an den Daten durchführen.
Die Angreifer haben normalerweise das gesamte Netzwerk aufgeklärt und verfügen vermutlich über einen besseren und aktuelleren Netzplan als Ihre eigenen Administratoren. In manchen Fällen etablieren die Angreifer im Netzwerk Brückenköpfe, welche als Einzige aktiv mit der Außenwelt kommunizieren. Andere kompromittierte Systeme kommunizieren nur mit den Brückenköpfen. Wird jetzt nur der Brückenkopf bereinigt, weil nur dieser in den ersten Analysen aufgefallen ist, kann der Angreifer über eventuelle Hintertüren auf den anderen Systemen wieder die Kontrolle über Ihr Netzwerk zurückerlangen.
Das Management sollte frühzeitig informiert und diesem insbesondere die Dimension eines solchen Angriffes aufgezeigt werden.

3.2 Vorfallsbewältigung als Projekt

Die wenigsten Unternehmen haben Erfahrungen in der Bewältigung größerer Sicherheitsvorfälle. Daher existieren oft auch keine vorbereiteten Pläne und Strukturen, falls ein APT-Angriff festgestellt wird.
Die meisten betroffenen Firmen haben aber Erfahrungen mit der Durchführung von Projekten. Daher kann es sinnvoll sein, die Vorfallsbewältigung als Projekt aufzufassen und diese mit den Mitteln des Projektmanagements anzugehen.
Man kann den Ablauf der Vorfallsbewältigung grob in 3 Phasen einteilen.

// INHALT ENTFERNT

3.3 Der APT-Angriff ist Teil einer Kampagne.

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

- Unternehmen, die im gleichen Sektor tätig sind,
- Unternehmen, die eine bestimmte Technologie einsetzen,
- Unternehmen, die alle den gleichen Kunden, zum Beispiel im Verteidigungsbereich, haben.

Zusammengefasst nennt man solch eine Serie von Angriffen eine Kampagne.

//INHALT ENTFERNT
Für ein einzelnes Opfer eines solchen Angriffes ist es schwierig, selbst Anzeichen für eine Kompromittierung zu finden. Daher ist es unbedingt notwendig, dass Institutionen die einen APT-Angriff entdecken diesen an eine kompetente Stelle weitermelden, damit diese weitere mögliche Opfer informieren kann.

Abgewehrte Angriffe melden

Es ist wichtig, dass auch nicht erfolgreiche Angriffe an eine kompetente Stelle, wie das BSI gemeldet werden. Auch wenn Sie einen APT- Angriff abgewehrt haben, könnte der gleiche Angriff bei einem Ihrer Kunden, Partner oder Zulieferer erfolgreich verlaufen sein.

3.4 Kommunikation – Der Angreifer lauscht mit!

Bei einem APT-Angriff können Sie keinem System, welches sich im infizierten Netzwerk befindet, vertrauen. Sie müssen davon ausgehen, dass der Angreifer Zugriff auf alle Daten in diesem Netz hat, wie E-Mails, Kalender, VoIP-Anrufe sowie Dateien.

//INHALT ENTFERNT

Die Krisenkommunikation sollte daher über getrennte Netze („Out-of-Band“) erfolgen.

// INHALT ENTFERNT

Binden Sie frühzeitig relevante interne Stellen ein, zum Beispiel in Form eines Krisenstabes:

- Leitungsebene
- IT-Experten (IT-Support)
- Juristen (Haftung, Strafanzeige, weitere rechtliche Aspekte, ...)
- Datenschutzbeauftragter (für Logging)
- Personal- / Betriebsrat (wegen Zugriff auf Logdaten)

3.5 Externe Unterstützung

In der Regel besitzen selbst große Firmen nicht genug interne Expertise für die erfolgreiche Vorfallsbehandlung bei einem APT-Angriff. Für viele Institutionen ist es das erste Mal, dass sie mit einem APT-Angriff konfrontiert werden. Wenden Sie sich daher frühzeitig an externe Experten.

Es kann sein, dass Ihre Institution und Ihre Systeme gar nicht das finale Ziel der Angreifer sind, sondern nur Ausgangspunkt für weitere Angriffe. Dies hat zur Folge, dass die Systeme von Kunden, Zulieferern oder Partnern durch die Interaktion mit Ihrem Netzwerk vielleicht kompromittiert wurden. Ein Incident Handling, welches sich nur auf das eigene Unternehmen beschränkt, wäre dann nicht ausreichend.

Folgende Hinweise bezüglich externer Unterstützung gelten für Institutionen in Deutschland. In anderen Ländern müssen die entsprechenden lokalen Behörden kontaktiert werden.

Bundesamt für Sicherheit in der Informationstechnik (BSI)

Das BSI ist ein kompetenter Ansprechpartner im Fall eines APT-Angriffes. Es verfügt über fundierte Kenntnisse bei der Behandlung von APT-Angriffen. Bei folgenden Punkten kann Sie das BSI unterstützen:

- Besprechung von Maßnahmen
- Unterstützung durch vorbereitete Dokumente
- Vermittlung von (Forensik-)Experten
- Koordination des Informationsaustausches mit anderen Experten oder Betroffenen, z.B. über Indicators of Compromise (IoC)
- Unterstützung bei der Kontaktaufnahme mit dem entsprechenden Landes- oder Bundesamt für Verfassungsschutz

//INHALT ENTFERNT

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

Zur Kontaktaufnahme wenden Sie sich direkt an das Computer Emergency Response Team des Bundes (CERT-Bund)[2] im BSI.

Landesamt für Verfassungsschutz (LfV)

Das für Sie zuständige LfV ist Ihr Ansprechpartner bei einem Verdacht auf Wirtschaftsspionage in ihrem Netz. Die Zusammenarbeit mit dem LfV erfolgt vertraulich. Auch im LfV liegen Erkenntnisse zu anderen Fällen vor, die bei einer Meldung herangezogen werden können. Dadurch kann das LfV Zusammenhänge zwischen Vorfällen herstellen.

Polizeien

Bei einem APT-Angriff werden in der Regel mehrere Straftaten begangen, insbesondere solche nach §§ 202a, 202b, 202c, 303a und 303b StGB. Für den Fall, dass Sie den APT-Angriff zur Anzeige bringen wollen, können Sie Strafanzeige bei bei der Polizei stellen.

Die Bundesländer bzw. die zuständigen Landeskriminalämter haben für diese Zwecke Anlaufstellen eingerichtet, die Opfern von Cyber-Straftaten beratend zur Seite stehen und bei einer Anzeige unterstützen. Eine Liste der Anlaufstellen, sowie ein Broschüre zum Thema finden Sie auf den Webseiten der Allianz für Cybersicherheit[3].

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

Grundsätzlich empfehlen wir, Cyber-Angriffe zur Anzeige zu bringen.

Unternehmen mit Schwerpunkt Computerforensik

Allgemein ist bei der Auswahl eines Forensik-Unternehmens zu beachten, dass die Unternehmen unterschiedliche Analyseschwerpunkte haben. Die Bandbreite des Knowhows reicht dabei von der Analyse netzwerkbasierter APT-Angriffen bis hin zur Wiederherstellung von physisch zerstörten Festplatten.

2 https://www.bsi.bund.de/CERT-Bund
3 https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Meldestelle/ZAC/polizeikontakt.html

Das BSI arbeitet im Rahmen der Allianz für Cybersicherheit mit etablierten Unternehmen mit dem Schwerpunkt Computerforensik aus Deutschland zusammen.

4 Teil 2 – Technische Analyse

In diesem Kapitel werden technische Maßnahmen vorgestellt, mit denen man das Ausmaß des Angriffes eingrenzen kann.

4.1 Forensische Beweissicherung

//INHALT ENTFERNT

4.2 Antivirus Programme

Ein AV-Scanner erkennt in der Regel nicht die bei einem APT-Angriff eingesetzte Schadsoftware, da diese gerade so konstruiert wurde, nicht von der AV-Software beim Opfer entdeckt zu werden. Ein Virenscanner kann aber in manchen Fällen bei der Frage helfen, ob es sich um einen APT-Angriff oder eine normale Kompromittierung handelt.

Bevor auf Systemen im Livebetrieb ein manueller Suchlauf eines AV-Programms gestartet wird, sollte beachtet werden, dass dadurch in der Regel sehr viele wichtige Daten verändert werden, wie zum Beispiel die Zeitstempel des letzten Zugriffes auf eine Datei, welche für die spätere forensische Auswertung benötigt werden. Daher sollte ein System immer erst, wie in Kapitel 4.1 beschrieben, forensisch gesichert werden, bevor darauf weitere Maßnahmen durchgeführt werden.

4.3 Umgang mit Logdaten

//INHALT ENTFERNT

4.4 Netzwerkverkehr-Analyse

//INHALT ENTFERNT

4.5 Wo Verkehrs-/Inhaltsdaten erfassen?

//INHALT ENTFERNT

4.6 Wie loggen?

//INHALT ENTFERNT

4.7 Anmerkungen

//INHALT ENTFERNT

4.8 Praxishilfe

//INHALT ENTFERNT

4.9 Analyse – Wo beginnen?

//INHALT ENTFERNT

Erste Schritte

//INHALT ENTFERNT

APT Angriff oder nur „normale“ Infektion

//INHALT ENTFERNT

4.10 Bereinigung

//INHALT ENTFERNT

5 Schlussbemerkung / weiteres Vorgehen

Dieses Papier soll Betroffenen helfen, bei der Bewältigung eines APT-Angriffes keine Fehler in der Anfangsphase zu begehen, die später dazu führen, dass der Angriff nicht aufgeklärt oder bereinigt werden kann. Dieses Papier stellt aber nur den ersten Einstieg in das Incident Handling eines APT-Angriffes dar, welches sich über Wochen und ggf. sogar Monate erstrecken kann.

Das BSI verfügt über eine Reihe an weiteren Papieren, die bei der weiteren Bewältigung eines APT-Angriffes unterstützen. Diese sind im folgenden Kapitel aufgelistet und können Betroffenen auf Anfrage zugesendet werden.

Diese Papiere sind, genauso wie dieses Papier, Arbeitspapiere die aufgrund neuer Erkenntnisse und Erfahrungen ständig weiterentwickelt werden. Das BSI ist daher sehr an Rückmeldungen bezüglich der Inhalte der Papiere interessiert.

Darüber hinaus ist das BSI regelmäßig bei APT-Angriffen auf Bundesbehörden, kritische Infrastrukturen und Institutionen im staatlichen Interesse koordinierend und unterstützend bei Vorfällen eingebunden und verfügt daher ggf. über weitergehende Informationen zu dem Sie betreffenden APT-Angriff, wie Indicators of Compromise (IoCs).

Unternehmen, die einen APT-Angriff entdecken, egal ob dieser erfolgreich ist oder abgewehrt wurde, sollten sich daher an das BSI wenden.

6 Weitere Dokumente

Die Dokumente Nr.1 - Nr.3 werden durch CERT-Bund an Interessierte auf Nachfrage herausgegeben oder sind über die Allianz für Cyber-Sicherheit abrufbar.

Nr.	Titel	Auszug - Inhaltsverzeichnisse[4]
1	Vertrauliche Meldungen an das BSI - Spezielle Informationen zu Advanced Persistent Threats (APT) TLP Green	*Grundsätzliche Rahmenbedingungen*
		Handhabung der Daten im BSI
		Verteilerkreise
		Typische Daten
2	Advanced Threat Protection TLP Green	*Prävention und Detektion fortgeschrittener Angriffstechniken*
3	Hinweise für das Management Offen	*Betroffenheit*
		Wo findet die Spionage statt?
		Schäden
		Entscheidungen und Maßnahmen
		Hinweise an den Betriebs-/Personalrat
		Bekannt gewordene APT-Vorfälle

Die folgenden Papiere werden nur an ausgewählte Betroffene unter der Einstufung „TLP Amber“ auf Anfrage weitergegeben.

Nr.	Titel	Auszug - Inhaltsverzeichnisse
4	//INHALT ENTFERNT	*//INHALT ENTFERNT*
		//INHALT ENTFERNT
		//INHALT ENTFERNT
5	//INHALT ENTFERNT	*//INHALT ENTFERNT*
		//INHALT ENTFERNT
		//INHALT ENTFERNT
		//INHALT ENTFERNT

4 Anmerkung: Die weiteren Dokumente werden als Arbeitspapiere fortlaufend weiterentwickelt und ständig mit praktischen Erfahrungen angereichert. Die hier dargestellten Papiere und Auszüge aus den Inhaltsverzeichnissen dienen lediglich der Orientierung und spiegeln den Stand von Oktober 2015 wieder.

7 Anlagen

7.1 Vorbereitungen für externe Unterstützung

Wie in Kapitel 3.5 beschrieben, ist es für Unternehmen ohne eigenes APT-Forensik Team in der Regel ratsam, externe Unterstützung für die Analyse des Vorfalls hinzuzuziehen.

Folgende Vorbereitungen Ihrerseits ermöglichen einem externen Forensik-Unternehmen schnell mit der Bearbeitung des Vorfalls zu beginnen:

//INHALT ENTFERNT

TLP WHITE //
~~**TLP AMBER**~~

7.2 Erklärungen zum Traffic Light Protokoll (TLP)

Dieses Dokument und die darin enthaltenen Informationen sind gemäß dem TLP eingestuft:

1) Was ist das Traffic Light Protokoll?

Das TLP ist ein von der OECD entworfenes Protokoll, welches die Weitergabe von sensitiven Informationen innerhalb eines Informationsverbundes regelt. Die vom Autor adressierten Empfänger dieses Dokumentes haben sich im Vorfeld schriftlich verpflichtet das TLP zu beachten und das Dokument entsprechend den "Ausführungsbestimmungen zum sicheren Informationsaustausch mit TLP“ zu verarbeiten, aufzubewahren, weiterzugeben und zu vernichten.

2) Welche Einstufungen existieren?

- **TLP-WHITE** : **Unbegrenzt**
  Abgesehen von urheberrechtlichen Aspekten dürfen Informationen der Stufe TLP-WHITE ohne Einschränkungen frei weitergegeben werden.
- **TLP-GREEN**: **Organisationsübergreifende Verteilung**
  Informationen in dieser Stufe dürfen innerhalb der Organisationen und an deren Partner frei weitergegeben werden. Die Information darf jedoch nicht veröffentlicht werden.
- **TLP-AMBER**: **Organisationsinterne Verteilung**
  Informationen in dieser Stufe dürfen innerhalb der Organisationen der Empfänger weitergegeben werden, jedoch nur auf der Basis „Kenntnis nur wenn nötig“. Der Informationsersteller muss zusätzlich beabsichtigte Einschränkungen der Weitergabe klar spezifizieren.
- **TLP-RED**: **Persönlich, nur für benannte Empfänger**
  TLP-RED-Informationen sind auf den Kreis der Anwesenden in einer Besprechung, einer Video-/Telefonkonferenz bzw. auf die direkten Empfänger bei schriftlicher Korrespondenz beschränkt. Eine Weitergabe ist untersagt. In den meisten Fällen werden TLP-RED-Informationen mündlich oder persönlich übergeben.

3) Was mache ich, wenn ich das Dokument an jemanden außerhalb des im TLP vorgegebenen Informationsverbundes weitergeben will?

Sollte eine Weitergabe an einen nicht durch die Einstufung genehmigten Empfängerkreis notwendig werden, so ist diese vor einer eventuellen Weitergabe durch den Informationsersteller nachvollziehbar zu genehmigen. Bei ausnahmsweiser Weitergabe im Rahmen einer bestehenden gesetzlichen Verpflichtung ist der Informationsersteller – nach Möglichkeit vorab – zu informieren.

4) Was passiert, wenn ich die Einstufung nicht beachte?

Bei Verstoß gegen die Regeln zur Weitergabe von Informationen erhält der Verpflichtete zukünftig nur noch TLP-White eingestufte Informationen aus dem Kreis der Verpflichteten.