Abwehr von Advanced Persistent Threats (APTs)

Kopf nicht in den Sand

APTs sind gezielte komplexe Angriffe. Nicht immer sind Definition und Kontext allerdings wirklich korrekt – was dazu führen kann, dass Unternehmen und Öffentliche Hand ihre IT-Sicherheitsstrategie nicht optimal ausrichten. Der Beitrag erläutert, welche Angreifer, Motive und Technik hinter dem Phänomen stecken können, wie die Dramaturgie solcher Angriffe abläuft, wie sich Angreifer verraten und wie man die APT-Abwehr optimiert.

Die Liste der Ziele, die bereits Opfer gezielter Angriffe wurden, wächst ständig, APTs werden zu einer immer größeren Bedrohung. Zu den bevorzugten Zielen zählen die Öffentliche Hand, die produzierende Industrie und Technologieführer aus dem Mittelstand, aber zunehmend auch Betreiber kritischer Infrastrukturen. Kein Unternehmen ist zu klein, um Opfer eines solchen Angriffs zu werden. Die Angreifer sind häufig hochqualifiziert und finanziell bestens dafür ausgestattet, mit hohem Aufwand Wirtschaftsspionage oder digitale Kriegsführung zu betreiben.

Wofür steht der Begriff „advanced" (fortgeschritten)? Er bezieht sich auf die Qualität der Angriffe: Diese sind gezielt aufgebaut, die Angreifer nutzen das gesamte Spektrum an logischen, physischen und sozialen Einfallstoren, und ein Angriff ist oft nur schwer nachvollziehbar.

Was ist mit „persistent" (anhaltend) gemeint? Während Angreifer normalerweise nach einem erfolgreichen Einbruch und Diebstahl schnell wieder das Weite suchen, nisten sich APT-Angreifer im Opfernetzwerk langfristig ein. Stuxnet zum Beispiel soll sich mehr als zwölf Monate im System aufgehalten haben, bis er entdeckt wurde, Red October sogar fünf Jahre. Ziel ist es, unbemerkt so tief wie möglich ins Netzwerk einzudringen, um zum Beispiel so viele wertvolle Daten wie möglich zu entwenden oder diese zu manipulieren.

Bei herkömmlichen Angriffen ist die Zahl der Opfer nicht eingegrenzt; APTs hingegen zielen meist nur auf einige wenige Opfer oder gar nur auf ein einziges. Die Angreifer spähen diese Ziele im Vorfeld genauestens aus.

Bei „konventionellen" Attacken steht oft nur eine Malware-Technik im Mittelpunkt; bei APT-Angriffen werden mehrere Methoden und Strategien häufig kombiniert und möglichst passgenau auf den jeweiligen Einsatzzweck zugeschnitten. Dazu gehören Spear-Phishing, Social Engineering, das Ausnutzen von Schwachstellen oder die Platzierung von Schadsoftware auf Websites, die die Mitarbeiter des Zielunternehmens häufig aufrufen (sogenannter „Watering Hole Attack" oder Wasserstellenangriff).

Was normale Cyberkriminelle interessiert, um im Netz Profit zu machen, zum Beispiel Zugangsdaten, ist für APT-Initiatoren nicht in erster Linie von Belang, sondern nur Mittel zum Zweck. Das Eindringen per Phishing dient APT-Angreifern lediglich als Sprungbrett, um tiefer ins System einzudringen und an das tatsächliche Hauptziel zu gelangen, zum Beispiel an die Patente eines Unternehmens.

Typisch für APT-Angreifer sind unternehmensähnliche organisatorische Strukturen bis hin zu Fachabteilungen, Lohnbuchhaltung und Netzwerk-Verantwortlichen. Auf der Fachebene gibt es Softwareprogrammierer, die statt herkömmlicher Apps eben Malware entwickeln. Auch die Spezialisierung auf bestimmte Plattformen wie Windows oder Linux ist üblich. Neben dem Programmiererteam, das die Software für die Angriffe implementiert, gibt es IT-Administratoren, die die für die Angriffe notwendige IT-Infrastruktur betreiben und pflegen. Dies ist durchaus eine Herausforderung, denn sie müssen nicht nur dafür sorgen, dass das System stabil, sondern auch möglichst intransparent bleibt und jede Nachverfolgbarkeit zu laufenden Angriffen weitestgehend ausgeschlossen ist.

Ein möglicher Verlauf

Es gibt keine typischen Angriffsvektoren oder Angriffsverläufe. Deshalb ist es relativ schwer für Unternehmen und Organisationen, sich davor zu schützen. Immer geht es darum, eine Organisation auszuspionieren, einen Host zu kompromittieren, Remote Access Tools (RATs) zu installieren, sich Administratorrechte einzurichten und Benutzerdaten zu entwenden sowie Zugriff auf relevante Daten zu erhalten. Auch wenn es vielen Angreifern gelingt, unterhalb des Radars zu arbeiten, hinterlässt nahezu jeder APT-Angriff Spuren und Hinweise auf dem System, in einigen Fällen auch in den Logmeldungen (mehr dazu weiter unten).

Ein möglicher Verlauf sieht wie folgt aus: Am Anfang kann ein Spear-Phishing-Angriff stehen, der eine Schadsoftware im Anhang verbirgt. Wird der Anhang geöffnet, nutzt dieser wiederum Schwachstellen in Office-Programmen oder anderer Software, um Dropper oder Malware nachzuladen, Hintertüren einzurichten oder temporäre Dateien einzuschleusen, die wiederum den permanenten Zugriff auf lokale Systeme ermöglichen. Ziel ist es, Passwörter zu entwenden und Tastatureingaben zu überwachen. In der Regel suchen Angreifer dann nach weiteren Sicherheitslücken in der IT-Infrastruktur, um an immer wertvollere Informationen zu gelangen.

Nach und nach etablieren sie über eine permanente Verbindung immer mehr zuverlässige Hintertüren und laden so Module nach, um das Unternehmen weiter auskundschaften und den Angriff adaptiv

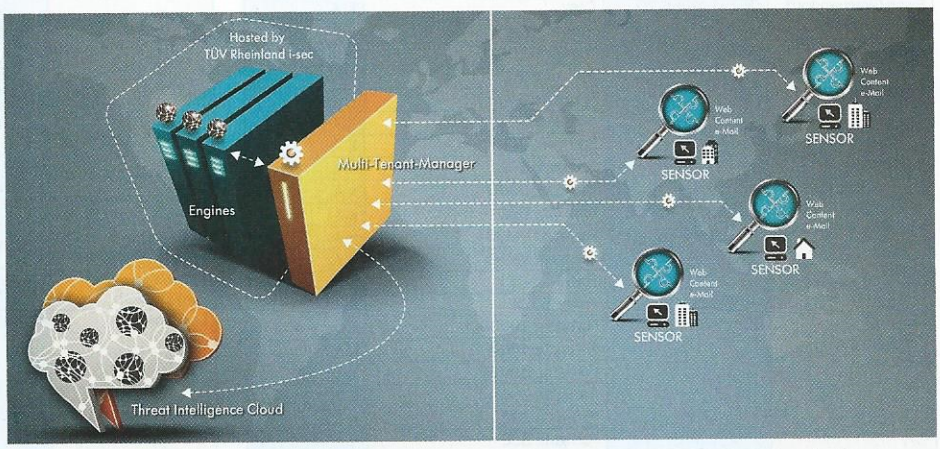
zu verschleiern. So können selbst Experten einen solchen Angriff nur sehr schwer nachvollziehen. Es gibt sogar Varianten, bei denen die Angreifer jedem Zielsystem eine eigene ID vergaben. So waren sie nicht nur in der Lage, das System genau zu kontrollieren, sondern konnten auch unterschiedlichste Formen von Malware passgenau einsetzen – unter Umständen auch als „Einmal-Version", um klassische Detektionssysteme noch besser zu unterlaufen.

Wie sich Angreifer verraten

Angreifer hinterlassen erfahrungsgemäß Fragmente ihres Schaffens auf einem Zielsystem, in Fachkreisen IOCs (Indicators of Compromise) genannt. Diese IOCs können vielfältig sein; häufig sind es Dateien, Skripte, Registry Keys oder andere Informationen. Ist die Malware nur im Speicher des Systems vorhanden (Memory-based Malware) und nicht auf einem Medium wie einer Festplatte persistent, steigt der Aufwand für die Generierung von IOCs.
Kommuniziert die Malware über eigene Kommunikationskanäle und erhält von einem externen C&C-Server (Command-and-Control-Server) Befehle, kann diese Kommunikation Spuren in Logmeldungen von Firewalls oder Proxies hinterlassen. So lässt sie sich zum Beispiel mittels eines SIEM-Systems (Security-Information- und Event-Management) auswerten. Nutzen Angreifer allerdings „legitime" Kommunikationskanäle wie Twitter (zum Übermitteln von Kommandos an die Malware) oder Dropbox (zur Datenexfiltration), sind die Erkennungsmöglichkeiten über die Loginformationen eingeschränkt. Gleiches gilt auch, falls die Malware nur dann aktiv wird und Netzwerkverkehr verursacht, wenn sie erkennt, dass das Zielsystem (etwa ein Notebook) sich außerhalb des Unternehmensperimeters befindet.

Die richtige Sicherheitsstrategie

Wie können sich Unternehmen vor APTs schützen? Die schlechte Nachricht zuerst: so gut wie gar nicht. Allerdings ist das kein Grund, jetzt jegliche Vorsicht fahren zu lassen. Im Gegenteil: Klassische Strategien, Konzepte und Schutzmaßnahmen haben nach wie vor ihre Berechtigung. Schließlich gibt es die gemeine Malware nach wie vor, und häufig verschaffen sich auch APT-Angreifer über typische Schwachstellen Zugang zum Unternehmensnetzwerk. Wichtig ist, dass Unternehmen akzeptieren, Opfer eines APTs werden zu können. Wer APTs nicht völlig schutzlos ausgeliefert sein will, muss seine IT-Sicherheitsstrategie regelmäßig überprüfen und ergänzende Maßnahmen treffen. Dies kann den Einsatz sensorbasierter Erkennungslösungen und die Einführung solider Incident-Response-Strukturen beinhalten, um einen möglichen Schaden schon im Keim ersticken und nachgelagerte Aufwände zur Beseitigung eines Angriffs möglichst zu verringern.



Für einen externen APT-Abwehr-Service positioniert ein Dienstleister (MSSP) Sensoren in Kundennetzwerken, die Analyse der IOCs erfolgt hingegen isoliert im RZ des Dienstleisters. Bild: TÜV Rheinland

Wichtig ist es, entsprechendes Know-how im Hause zu haben, also Experten, die in der Lage sind, Sicherheitsvorfälle in ihrer Kritikalität richtig zu bewerten und geeignete Abwehrmaßnahmen zu empfehlen. Ist das nicht der Fall, sind externe Spezialisten (Managed-Security-Service-Provider, MSSP) eine gute Alternative, die sich wirtschaftlich rechnet.
Es gibt es mehrere technische Möglichkeiten, um Angriffe aufzuspüren. Entscheidend ist die Erkennung relevanter Spuren im Netzwerk und auf den wichtigen Systemen selbst. Hierzu muss die entsprechende Sensorik an den richtigen Stellen platziert sein. Nützlichen Input kann hier ein GRC-System (Governance, Risk, and Compliance) liefern. Auf der Basis diverser Vorgaben und den Ergebnissen von Risikoanalysen lassen sich damit Prioritäten für die verschiedenen Assets und Asset-Gruppen ableiten. Ziel ist es, Angriffe auf unternehmenskritische Assets zuerst erkennen zu können. Als Sensor bieten sich vielfältige Quellen an: Denkbar ist beispielsweise die Überwachung von Netzübergangskomponenten wie Firewalls, IDS/IPS oder Web- und Mail-Proxy-Systemen sowie der Systeme selbst (zum Beispiel Windows-Server inklusive Middleware und Applikationen), zudem Einsatz dedizierter APT-Sensorik.
Gerade mit solcher Sensorik geht man im Besonderen auf die aktuelle Bedrohungslage ein, da eine technische Erkennung von Anomalien in einem bestimmten Maß möglich ist – diese jedoch weiter qualifiziert werden muss. Hier können externe Spezialisten wertvolle Hilfe leisten, indem sie die relevanten Informationen verschlüsselt in ihr eigenes Rechenzentrum ausleiten, wo APT-Experten dann in einer isolierten Umgebung eine Analyse durchführen. Stellt sich heraus, dass das Unternehmen Ziel eines Angriffs ist, begleitet der MSSP die interne IT des Unternehmens bei der Qualifizierung und der Abwehr sowie der Entwicklung einer nachhaltigen Sicherheitsstrategie. Idealerweise integriert man die spezielle APT-Sensorik wie auch die herkömmliche Sensorik in einem SIEM-System. Ziel ist es dabei, ein zentrales Security Cockpit zu etablieren.

Thomas Mörwald/wg

Thomas Mörwald ist Senior Consultant Information Security and Application Services beim TÜV Rheinland, www.tuv.com.