Cyberangriffe verstehen

Die Cyber Kill Chain

Adaptive Defense

pandasecurity.com/intelligence-platform/

Inhaltsverzeichnis

1. Einführung

Die sich häufig ändernde Bedrohungslandschaft sowie die zunehmende Professionalität und Zielgerichtetheit der Angreifer erfordern eine Weiterentwicklung von Sicherheitspraktiken hin zu einer Kombination aus **Prevention, Detection und Response.**

Die meisten Unternehmen setzen bereits heute Technologien ein, um **bekannte Angriffe** zu entdecken. Was in der Vergangenheit als schwierig angesehen wurde, ist die Abwehr **unbekannter Attacken**, die speziell darauf ausgerichtet sind, die neuesten Schutzmaßnahmen zu umgehen, indem Signaturen und Verhaltensmuster verändert werden.

Viele Unternehmen haben erhebliche Investitionen getätigt, um mit eigenen IT-Security-Abteilungen potentielle Bedrohungen zu suchen und zu identifizieren. Oder sie haben diese Aufgabe an Managed Service Provider delegiert, deren Tätigkeit unter anderem die stetige Weiterentwicklung der Abwehrtechniken und die Suche nach besseren Tools und Möglichkeiten zum Schutz der digitalen Ressourcen umfasst.

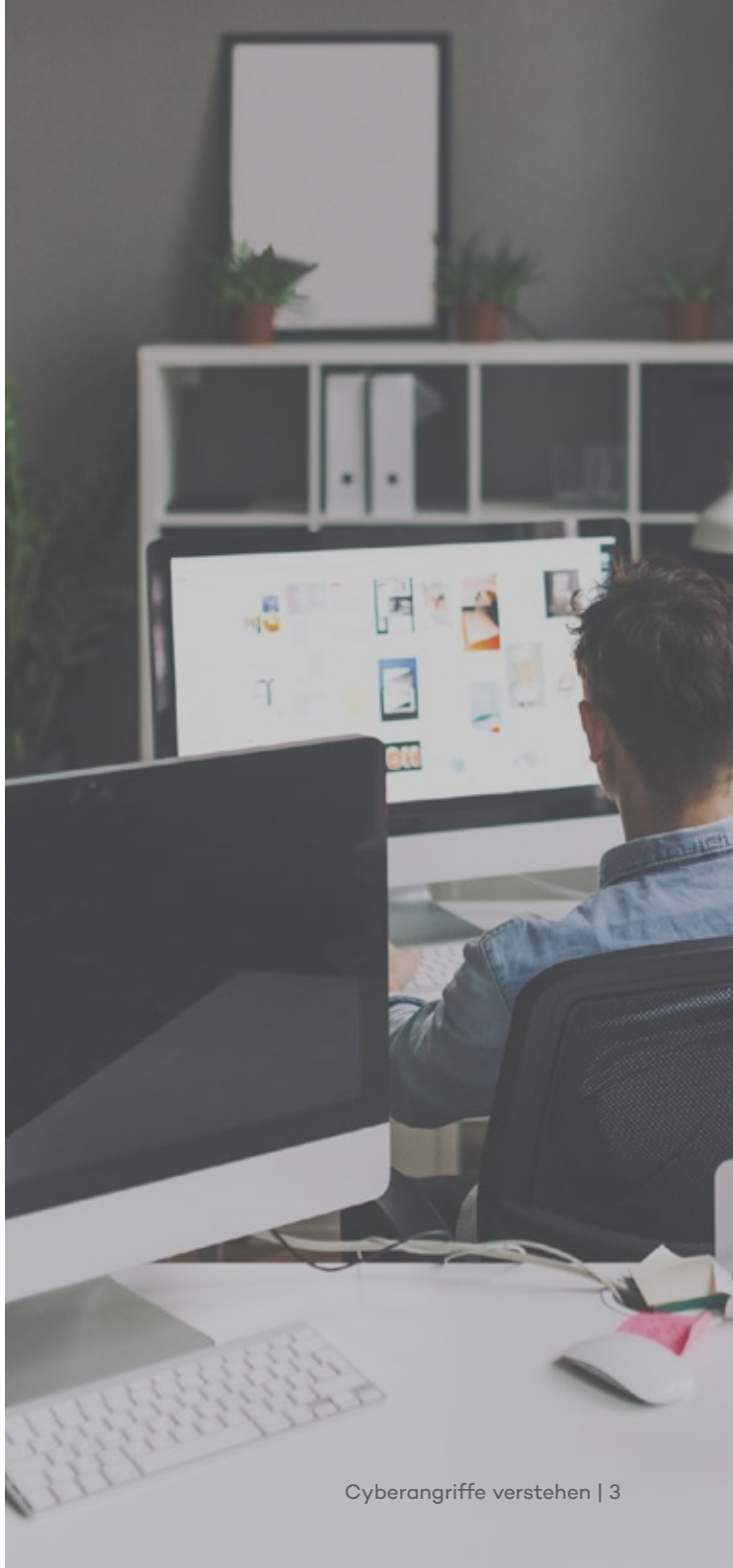
Zwei Dinge sind in diesem Zusammenhang sowohl für die Unternehmen als auch für die Provider von essentieller Bedeutung: Erstens, zu verstehen, wie die Cyberkriminellen arbeiten. Zweitens, die Erarbeitung eines Plans zur Verteidigung des eigenen Unternehmens. Dieser sollte sich an dem Lifecycle einer Cyberattacke orientieren und festlegen, wie eine Attacke entdeckt, gestoppt und unterbrochen werden kann, wie sich das Unternehmen von einer möglichen Attacke erholt und wo die Sicherheitsmaßnahmen verstärkt werden müssen.

Das vorliegende Whitepaper soll IT-Administratoren und Cyber Security Teams dabei helfen, das bekannte Cyberangriff-Lifecycle-Modell, die sogenannte Cyber Kill Chain (CKC), sowie seine Erweiterung auf das gesamte Netzwerk zu verstehen.

Die Cyber Kill Chain ist ein ausgezeichnetes Tool, um zu verstehen, wie Unternehmen die Verteidigungsfähigkeit ihrer IT-Umgebung maßgeblich erhöhen können, indem sie Bedrohungen in jeder Phase des Lifecycles der Attacke erkennen und stoppen. Die Kill Chain demonstriert, dass wir die Kette „nur“ an irgendeinem Punkt des Prozesse stoppen müssen, um die Attacke abzubrechen, während die Kriminellen alle Phasen durchlaufen müssen, um erfolgreich zu sein.

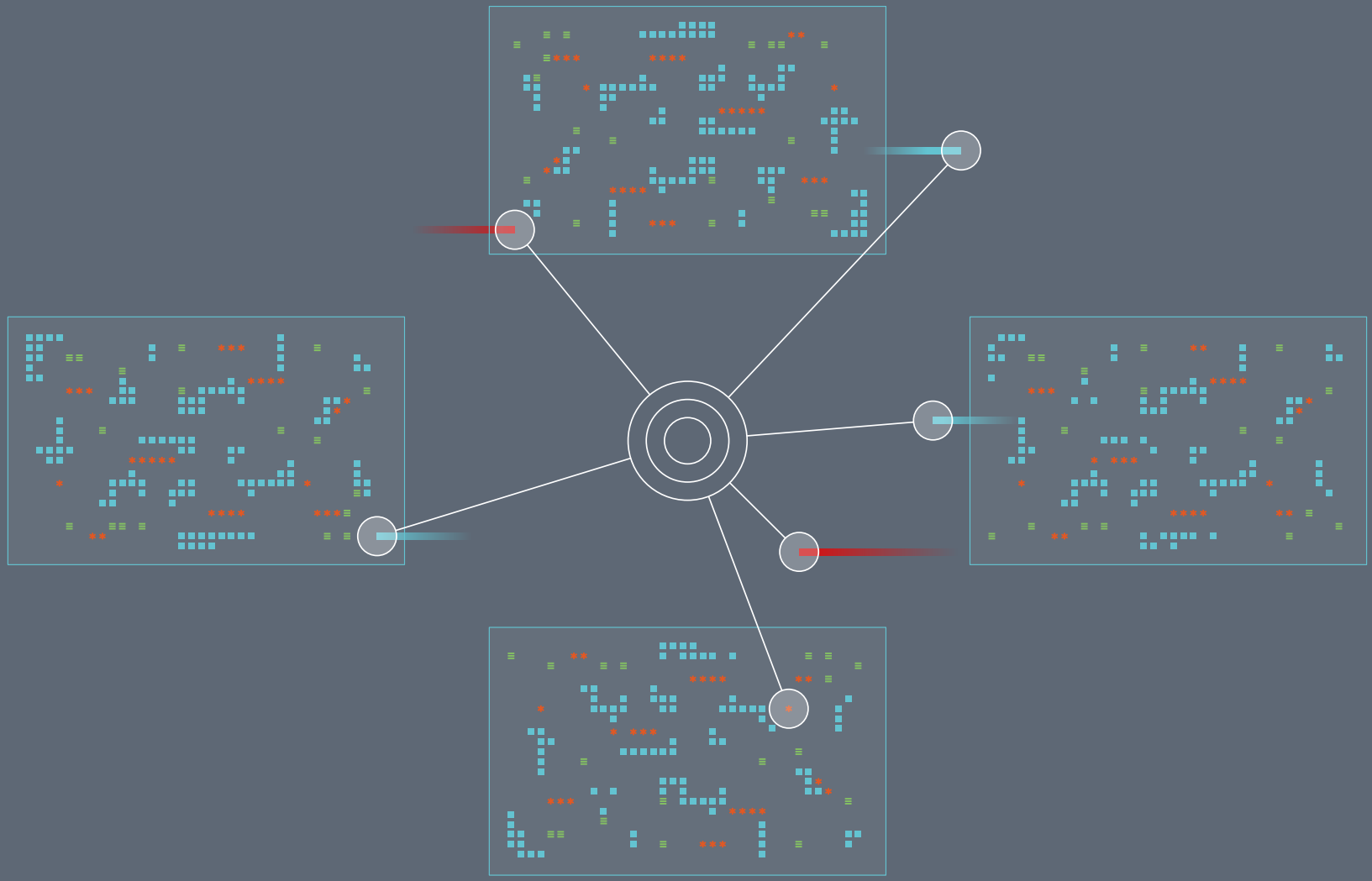
Es ist wichtig sich zu vergegenwärtigen, dass wertvolle Vermögenswerte eines Unternehmens – nämlich das spezielle Knowhow und sensible Daten – auf dessen Endpoints und Servern gespeichert werden, und dies manchmal unkontrolliert.

Da alle Angreifer bis zu den Endpoints vordringen wollen, um Zugriff auf die wichtigen Assets der Unternehmen zu erlangen, reduziert das Stoppen der Kriminellen am Endpoint-Level automatisch die Wahrscheinlichkeit des Erfolges aller Cyberattacken. Gleichzeitig werden die Bemühungen, die Kette zu durchbrechen, vereinfacht und die Effizienz sowie die Effektivität der Sicherheitsmaßnahmen werden erheblich erhöht.



Panda Adaptive Defense hilft Unternehmen sowie ihren internen oder externen Sicherheitsteams dabei, Bedrohungen zu entdecken und auf sie zu reagieren – egal an welcher Stelle im Cyber-Attack-Lifecycle die Bedrohungen den Endpoint erreichen.

Der Managed Service bietet zudem detaillierte Informationen über die Bedrohungen, damit Unternehmen mehr über die Angreifer erfahren und ihre Verteidigung verbessern können.



2. Die Cyber Kill Chain verstehen

Das Cyber-Kill-Chain-Rahmenkonzept wurde ursprünglich vom US-amerikanischen Rüstungs- und Technologiekonzern Lockheed Martin Corporation veröffentlicht, als Teil seines ‚Intelligence Driven Defense®'- Modells[1] zur Identifizierung und Prävention von Cyberattacken.

Das Modell ermittelt, was die Angreifer durchführen müssen, um ihr Ziel zu erreichen: Das Netzwerk ins Visier nehmen, Daten herausfiltern, Sicherung des Fortbestehens der Malware im Unternehmen.

Das Modell zeigt, dass die Angriffskette unterbrochen wird, egal in welcher Phase man die Angreifer stoppt. Angreifer müssen jedoch alle Phasen vollständig durchlaufen, um erfolgreich zu sein. **Fazit:** Wir als Verteidiger brauchen sie nur an einem beliebigen Punkt zu blockieren, um Erfolg zu haben.

Im nächsten Abschnitt werden wir sehen, dass der Endpoint ein unvermeidlicher Punkt ist, den alle erfolgreichen Attacken durchlaufen müssen. Deshalb steigt die Chance, einen Cyberangriff zu unterbrechen, wenn wir ihn an genau dieser Stelle stoppen. Die Erfolgsrate ist höher, je früher die Angriffe gestoppt werden.

Außerdem sind jedes Eindringen und die Spuren, die der Angriff hinterlässt, eine Chance, mehr über unsere Gegner zu erfahren und ihre Hartnäckigkeit zu unserem Vorteil zu nutzen. **Ein besseres Verstehen der Kriminellen und ihrer Spuren ermöglicht eine effektivere Gestaltung der Sicherheitsmaßnahmen.**

Die Cyber Kill Chain zeigt die sieben Phasen, die die Cyberkriminellen durchlaufen müssen, um ihre Angriffe auszuführen:

Reconnaissance

Dieses Stadium kann bezeichnet werden als die Phase der Zielauswahl und des Sammelns von Informationen über das Zielobjekt, wie Arbeitsroutinen, genutzte Technologie, Organisationsstrukturen, E-Mail-Adressen usw.

Der Angreifer sucht im Wesentlichen nach Antworten auf diese Fragen: „Welche Angriffsmethode wird mit den höchsten Erfolgschancen funktionieren?“ „Welche lässt sich in Bezug auf den Einsatz unserer Ressourcen am einfachsten ausführen?“

Weaponization

Hierbei geht es um die Auswahl des passenden Angriffsweges und der geeigneten Werkzeuge. Dieser kann viele Formen haben: Ausnutzung von Webanwendungen, serienmäßige oder maßgeschneiderte Malware, Schwachstellen in zusammengesetzten Dokumenten (PDF, Office und andere Dokumentenformate) oder ‚Watering Hole Attacks‘[2].

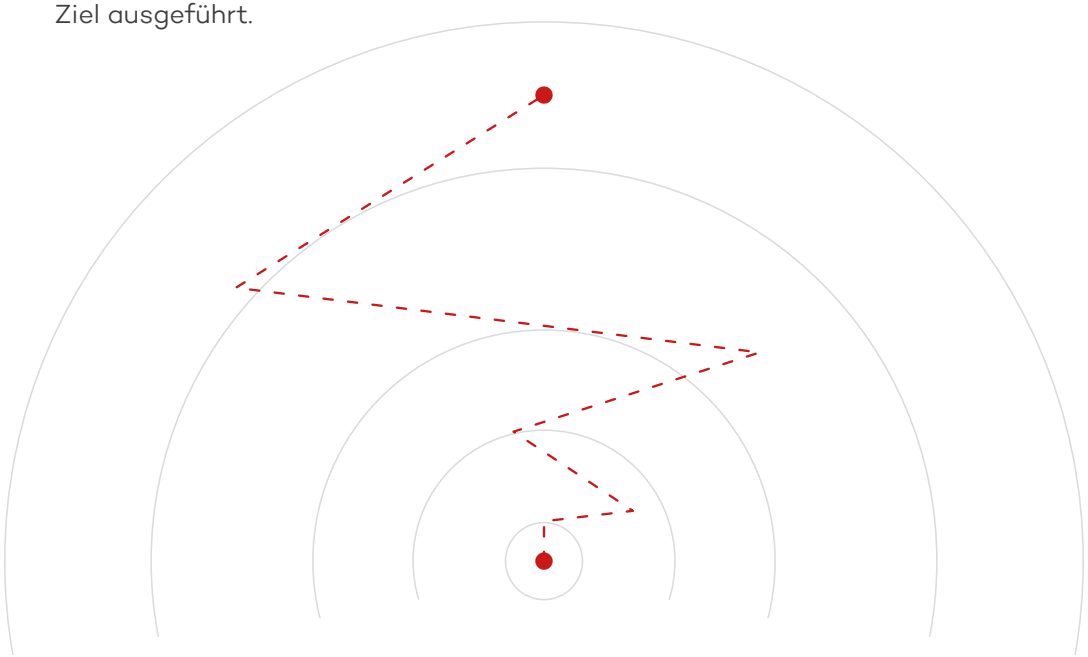
Diese werden im Allgemeinen mit opportunistischen oder sehr speziellen Informationen über das Ziel ausgeführt.

Delivery

Die Übertragung der schädlichen Inhalte wird entweder vom Ziel initiiert (z. B. wenn ein Anwender auf einer schädlichen Webseite surft, wobei Malware übertragen oder eine schädliche PDF-Datei geöffnet wird) oder vom Angreifer selbst (SQL-Einschleusung oder Gefährdung des Netzwerkdienstes).

Exploitation

Der Zugriff erfolgt gewöhnlich durch die Ausnutzung einer bekannten Schwachstelle, für die kurz zuvor ein Patch zur Verfügung gestellt wurde. Obwohl Zero-Day-Angriffe vorkommen, ist es in der Regel eher selten, dass die Angreifer einen derartigen Aufwand betreiben.



Installation

Die Schadsoftware setzt sich auf den Endpoints fest, auf die sie zugreifen konnte. Dabei agiert die Malware normalerweise im Verborgenen, so dass der Angreifer die Anwendungen kontrollieren kann, ohne dass dieses vom Unternehmen bemerkt wird.

Command-and-Control

In dieser Phase nimmt die Malware Kontakt zum Command-and-Control-Server auf. Die Angreifer suchen und öffnen dabei Kommunikationskanäle wie zum Beispiel DNS, Internet Control Message Protocol (ICMP), Webseiten und soziale Netzwerke, um die „Opfer“ aus der Ferne steuern zu können.

Actions on Objectives

Mit dieser finalen Phase erreichen die Angreifer ihr eigentliches Ziel: Sie kompromittieren Dateien oder Endpoints, um sich im angegriffenen Unternehmensnetzwerk festzusetzen. Dann werden Maßnahmen ergriffen, um weitere Ziele zu identifizieren und die kriminellen Aktivitäten in der angegriffenen Firma auszuweiten: Je nach Angreifer werden sensible Daten gesammelt und extrahiert, Systeme zerstört, Daten gestohlen und überschrieben etc.

Die Cyber Kill Chain (CKC) wird dann wiederholt. Hierbei gilt es zu verstehen, dass die CKC zyklisch abläuft und nicht linear.

Wenn ein Angreifer in ein Netzwerk eindringt, startet er die CKC erneut, um das Netzwerk weiter auszukundschaften und laterale Bewegungen auszuführen.

Ein weiterer wichtiger Punkt ist, dass die Angreifer trotz gleicher Methodik (Phasen) für die einzelnen Schritte der internen Kill Chain andere Techniken nutzen, als wenn der Angriff von außerhalb gestartet wird. Der Angreifer wird also zum Insider, zu einem User mit Privilegien. Dies verhindert, dass die Sicherheitsteams eines Unternehmens den Angriff vorhersehen und erkennen, dass dieser sich bereits in einer fortgeschrittenen Phase der Cyber Kill Chain befindet.

Externe Cyber Kill Chain

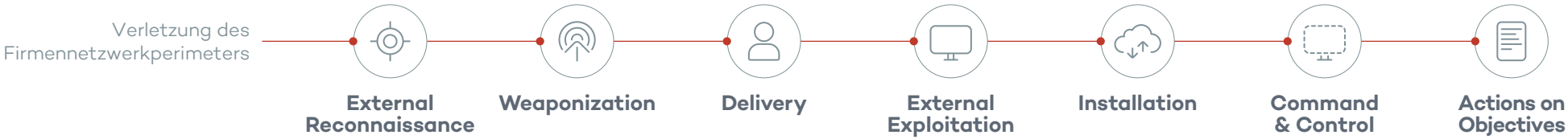


Abb. 1: Diagramm der Phasen in der Cyber Kill Chain vom Perimeter zum Endpoint. Die Externe Cyber Kill Chain

3. Die erweiterte Version der Cyber Kill Chain

Die Cyber Kill Chain ist ein zyklischer und nicht-linearer Prozess, bei dem der Angreifer ständige laterale Bewegungen innerhalb des Netzwerkes ausführt. Die Phasen, die innerhalb des Netzwerkes ablaufen, sind dieselben wie die, welche für den ursprünglichen Angriff von extern genutzt wurden, obwohl andere Techniken und Taktiken verwendet werden.

Die Kombination aus der externen und der internen Cyber Kill Chain wird in der Branche ‚Erweiterte Cyber Kill Chain' genannt. Das bedeutet, dass weitere Schritte zur externen Cyber Kill Chain hinzugefügt werden, wobei die Phasen gleich bleiben und eben nur intern ablaufen. So wird die externe Cyber Kill Chain ergänzt durch die interne Cyber Kill Chain mit ihren eigenen Phasen: Interne Erkundung, interne Bewaffnung, interne Zustellung usw.

Jede Phase des Angriffs kann, wenn sie erst einmal im Netzwerk des Opfers ist, von wenigen Minuten bis zu mehreren Monaten dauern, einschließlich einer Wartezeit, während der der Angreifer auf den optimalen Moment wartet, um die letzte Phase des Angriffs zu starten und so den maximalen Profit aus der Attacke zu ziehen.

Die Reconnaissance- und Weaponization-Phasen können Monate dauern. Es ist schwierig, diese Phasen zu unterbrechen, da sie ohne direkte Verbindung zum Angreifer ausgeführt werden.

Deshalb ist es von besonderer Wichtigkeit, dass die Sicherheitsmaßnahmen auf den Endpoints alle Anwendungen permanent analysieren und überwachen, die auf den Geräten laufen. Auf diese Weise wird die Arbeit der Angreifer erheblich erschwert, was die Attacke für sie letztlich unprofitabel macht.

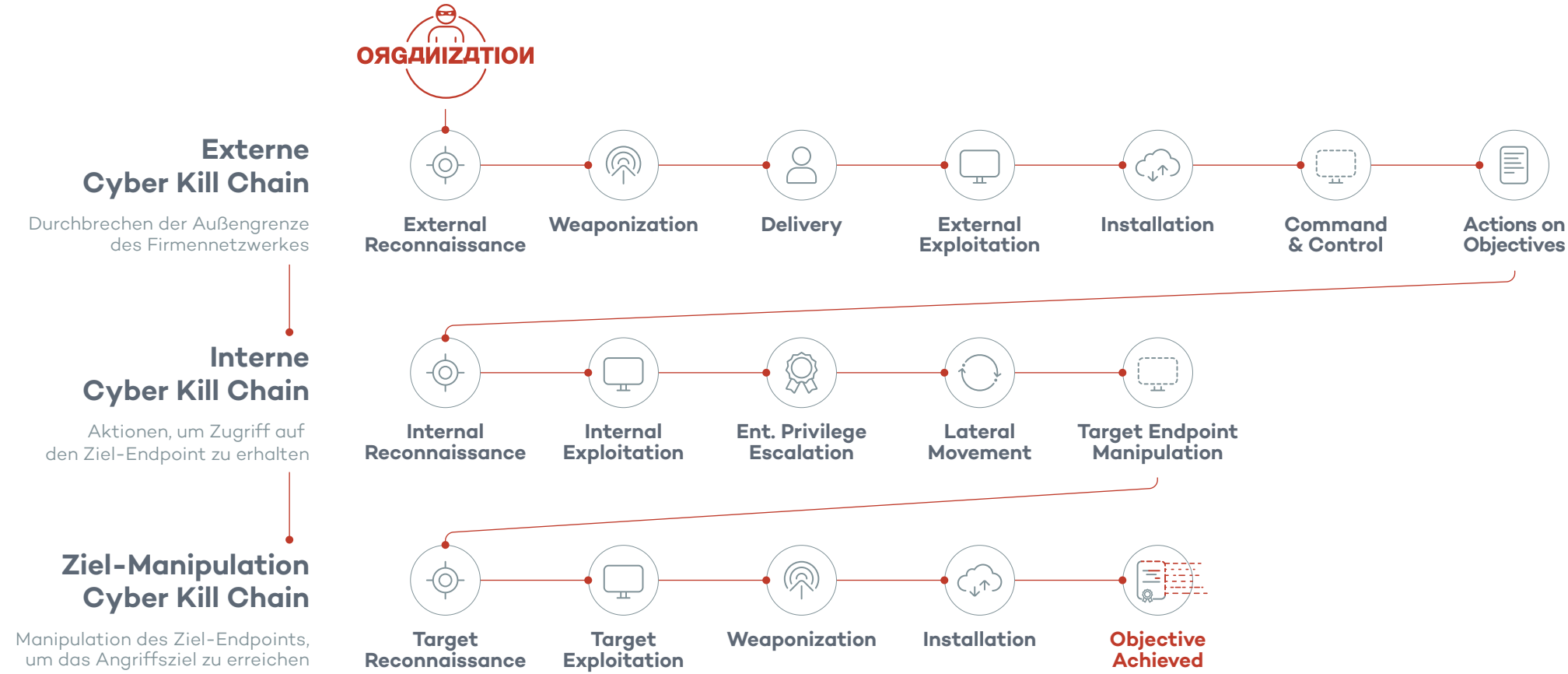
Internal Reconnaissance

In dieser Phase haben die Angreifer Zugriff auf einen einzigen Endpoint eines Anwenders. Sie werden diesen nach lokalen Dateien, Netzwerkfreigaben sowie Browser-Verläufen durchsuchen und auf Wikis und SharePoint zugreifen. Ziel ist es, herauszufinden, wie dieser Rechner genutzt werden kann, um das Netzwerk kennenzulernen und an wertvolle Daten und Informationen heranzukommen.

Internal Exploitation

Durch die Ausnutzung von fehlenden Patches, Schwachstellen in Webanwendungen, Sendeprotokollen, Spoofing oder Standardanmeldedaten erfolgt der interne Zugriff. Die Angreifer gelangen so von den Workstations zu den Servern, indem sie Rechte ausweiten, laterale Bewegungen innerhalb des Netzwerkes durchführen und individuell anvisierte Rechner manipulieren.

Abbildung 2. Die Erweiterte Cyber Kill Chain. Aktionen, um Zugriff auf den Ziel-Endpoint zu erhalten und Endpoint-Manipulation, um das Ziel zu erreichen.



4. Panda Adaptive Defense und die Cyber Kill Chain

Angreifer haben bestimmte Ziele und sind bereit, eine gewisse Menge an Ressourcen aufzuwenden, um diese zu erreichen. Wenn jedoch der vorhandene Endpoint-Schutz den Aufwand in die Höhe treibt – sei es nun finanziell, personell oder zeitlich –, sodass die Ausgaben letztlich höher sind als der zu erwartende Gewinn, werden die Erfolgsaussichten geringer oder die Angreifer werden das Unternehmen gar nicht erst angreifen.

Daher müssen sich alle Unternehmen die Frage stellen, was passieren würde, wenn der Angreifer Zugriff auf das interne Firmennetzwerk, Benutzernamen und Passwörter, alle Dokumentationen und Spezifikationen der Netzwerkgeräte, Systeme, Backups und Anwendungen hätte und sie sofort reagieren müssten.

Das übergeordnete Ziel jeder Endpoint-Security-Strategie sollte es sein, ein gut gerüstetes Unternehmen aufzubauen. Den Angriff als solchen kann sie zwar nicht verhindern, aber Attacken werden häufiger und in früheren Phasen gestoppt.

Eines der Ziele ist es, effiziente Verteidigungsmechanismen für die jeweiligen Phasen der erweiterten Cyber Kill Chain zu haben, um die Angriffe zu verlangsamen, ihre Fortführung zu verteuern und es den Angreifern so schwer wie möglich zu machen, zur jeweils nächsten Phase überzugehen.

Die Sicherheitsstrategie von Unternehmen sollte zudem berücksichtigen, wie eine Attacke ausgeführt wird, sowohl von außen als auch insbesondere von innen, da die Angreifer zu Insidern werden, wenn sie erst einmal im Netzwerk sind und Zugriff auf die Endpoints haben.

Auf der Basis der Cyber Kill Chain können Unternehmen ihre vorhandene Cyber-Abwehrstrategie analysieren und durch moderne Technologien erweitern, welche nicht nur verhindern können, dass die Angreifer Zugriff auf die Endpoints erlangen, sondern auch in der Lage sind, diese in jeder möglichen Phase der internen Cyber Kill Chain zu stoppen.

Die Analyse der eigenen Verteidigungsstrategie anhand des erweiterten CKC-Modells zeigt, wie das Unternehmen den Angriff während der verschiedenen Phasen verhindern, entdecken und unterbrechen sowie Systeme wiederherstellen kann.

Mit Adaptive Defense und Panda Adaptive Defense 360 bietet Panda Security zudem **einen Managed Service, der in der Lage ist, die hochentwickeltsten Angriffstechniken und -taktiken in jeder Phase der erweiterten Cyber Kill Chain zu entdecken und zu verhindern.**

5. Die Grundpfeiler von Adaptive Defense und Adaptive Defense 360

Abwehr bekannter Malware

Nach bekannten Bedrohungen zu suchen, wird nicht vor ihren neuen Varianten oder anderen unbekannten Attacken schützen. Wenn die Suche nach bekannten Bedrohungen jedoch durch zusätzliche Sicherheitslevel erweitert wird, können bekannte Bedrohungen präventiv gestoppt werden, wenn sie an den Endpoint übertragen werden. Panda Adaptive Defense 360 nutzt eine über Jahrzehnte aufgebaute cloud-basierte Sammlung an Reputationsservices (Pandas Collective Intelligence), um bekannte Bedrohungen in der Übertragungsphase in Echtzeit zu stoppen.

Fortschrittliche Malware-Erkennung

Panda Adaptive Defense und Panda Adaptive Defense 360 erkennen und blockieren dank seines auf drei Prinzipien basierenden Sicherheitsmodells zusätzlich unbekannte Malware und gezielte Angriffe: ständige ausführliche Überwachung aller auf den Endpoints laufenden Prozesse, automatische Klassifizierung dieser Prozesse mittels Maschinenlerntechniken auf einer cloud-basierten Plattform und die Möglichkeit, dass ein fachkundiger Techniker das Verhalten eines Prozesses analysiert, sollte dieser nicht automatisch klassifiziert werden können.

Dynamische Exploit-Erkennung[3]

In der Zugriffsphase der erweiterten Cyber Kill Chain nutzen Angreifer Exploits, um Schwachstellen auf Code-Level anzugreifen, damit sie in Anwendungen und Systeme eindringen sowie Malware installieren und ausführen können. Internet-Downloads sind ein üblicher Vektor für die Ausführung von Exploit-Attacken. Panda Adaptive Defense und Panda Adaptive Defense 360 bieten dynamische Anti-Exploit-Fähigkeiten, um sowohl vor anwendungsbasierten als auch speicherbasierten Angriffen zu schützen.

Panda Adaptive Defense und Panda Adaptive Defense 360 erkennen und blockieren die Techniken, die von Angreifern während der Zugriffsphase verwendet werden – zum Beispiel: Heap-Spray-Angriffe, Stack Pivoting, ROP-Attacken und Änderungen an den Speicherrechten. Darüber hinaus erkennen sie unbekannte Attacken dynamisch, indem sie alle auf den Geräten laufenden Prozesse permanent überwachen, Daten mittels Maschinenlernalgorithmen in der Cloud abgleichen und so in der Lage sind, jeden bekannten und unbekannten Versuch der Ausnutzung zu stoppen.

Adaptive Defense Anti-Exploit-Technologien stoppen den Angreifer in einer frühen Phase der internen Attacke, indem sie erkennen, wenn vertrauenswürdige Anwendungen oder Prozesse kompromittiert werden.

Schadensminderung

Ein Endpoint-Schutz der nächsten Generation muss Angreifer während der verschiedenen Phasen der Cyber Kill Chain präventiv abwehren bzw. diese entdecken. Jedoch muss der Erkennung eine schnelle Schadensminderung in den Anfangsphasen der Kill Chain folgen.

Panda Adaptive Defense 360 entschärft den Angriff automatisch und frühzeitig, indem es die Malware unter Quarantäne stellt, einen kompromittierten Prozess abbricht oder das System vollständig herunterfährt, um den Schaden zu minimieren.

Wiederherstellung

Während ihrer Ausführung erstellt, modifiziert oder löscht die Malware oft Systemdateien und Registry-Einstellungen und verändert die Konfigurationseinstellungen.

Diese Veränderungen und Überbleibsel, die zurückgelassen werden, können Systemfehler und Instabilität verursachen oder sogar eine Tür für neue Attacken öffnen.

Panda Adaptive Defense 360 stellt den Zustand wieder her, den die Endpoints vor der Malware-Infektion hatten.

Forensik

In der sich ständig ändernden Bedrohungslandschaft und angesichts des raffinierten und zielgerichteten Verhaltens der Angreifer sollte keine Sicherheitstechnologie behaupten, zu 100 Prozent effektiv zu sein. Deshalb ist die Fähigkeit, Endpoint-Forensik in Echtzeit und mit maximaler Transparenz zu bieten, ein Muss.

Die Cybersicherheitsteams in Firmen müssen einen Plan haben, wie sie gemeldete Sicherheitsverletzungen bearbeiten und wann diese gegebenenfalls den Strafverfolgungsbehörden gemeldet werden müssen.

Panda Adaptive Defense und Panda Adaptive Defense 360 bieten klaren und frühzeitigen Einblick in schädliche Aktivitäten im gesamten Unternehmen. Aufgrund dieser Transparenz können Sicherheitsteams schnell das Ausmaß einer Attacke beurteilen und entsprechende Maßnahmen ergreifen.

Abbildung 3.
Diagramm des Angriffs-Lifecycles anhand forensischer Analyse.

Abbildung 4. Adaptive Defense 360 Sicherheitssäulen während der erweiterten Cyber Kill Chain.

Literatur-verzeichnis

- Lockheed Martin's Cyber-Kill Chain: http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LMWhite-Paper-Intel-Driven-Defense.pdf
- Sean T. Mallon, Strategic Cybersecurity Leader & Executive Consultant, at Black Hat 2016: Extended Cyber kill chain
- Mitre's Cybersecurity Threat-Based Defense
- Microsoft's Security Development Life Cycle
- Gartner Research, G00298058, Craig Lawson, 07 April 2016

---

[1] Eric M. Hutchins, Michael J. Cloppert und Rohan M. Amion, Ph.D., Intelligence-Driven Computer Network Defense sachkundig durch die Analyse von Adversary Campaigns und Intrusion Kill Chains.

[2] **Watering Hole Attack**. Eine spezielle Art der gezielten Attacken, bei der das Opfer zu einer bestimmten Gruppe gehört (Organisation, Branche oder Region). Bei dieser Attacke vermutet oder beobachtet der Angreifer, welche Webseiten die Gruppe oft besucht, und infiziert eine oder mehrere von diesen mit Malware. Irgendwann werden einige Mitglieder der Zielgruppe infiziert.

Die Malware, die für diese Attacken verwendet wird, sammelt typischerweise Informationen über die Anwender. Angreifer, die spezielle Informationen suchen, greifen möglicherweise nur Anwender mit einer bestimmten IP-Adresse an. Dies erschwert es, die Angreifer zu entdecken und zu erforschen. Der Name ist von den Raubtieren in der Natur abgeleitet, die an Wasserlöchern auf eine Gelegenheit warten, ihre Beute anzugreifen.

Auf Webseiten zu bauen, denen die Gruppe vertraut, macht diese Strategie effizient, auch bei Gruppen, die nicht anfällig sind für Spear Phishing und andere Formen des Phishings.

[3] **Dynamische Exploit-Erkennung** ist die innovative Technologie von Panda Security, die auf der Überwachung aller Prozesse basiert, die auf den Endpoints oder Servern laufen und in der Cloud mithilfe von Maschinenlerntechnologien analysiert werden, die darauf ausgerichtet sind, Versuche, vertrauenswürdige Anwendungen auszunutzen, zu erkennen.

Das Ziel dieser neuen Technologie ist es, Angriffe auf Workstations und Servern bereits in der Anfangsphase der Cyber Kill Chain zu stoppen. Angreifer in Schach zu halten und sie in solch einem Ausmaß am Zugriff auf das Gerät zu hindern, dass die Profitabilität der Attacke leidet, wird sie von weiteren Versuchen abschrecken und somit zu einer höheren Erkennungsrate führen.

Weitere Informationen unter:

pandasecurity.com/de/business/

Rufen Sie uns an:

02065 961-200

Kontaktieren Sie uns per E-Mail:

vertrieb@de.pandasecurity.com

panda