Was Sie über Cyberangriffe wissen sollten

watchguard.com

panda
a WatchGuard brand

Index:

1.Einführung

Die häufig wechselnde Bedrohungslandschaft sowie die Häufigkeit, Raffinesse und Zielgerichtetheit von Angriffen machen eine Weiterentwicklung von Sicherheitspraktiken hin zu einer Kombination aus Prevention, Detection und Response notwendig.

Die meisten Unternehmen setzen bereits heute Technologien ein, um bekannte Angriffe zu entdecken, von denen einige trotzdem durchkommen. 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 potenzielle Bedrohungen ausfindig zu machen. Andere haben diese Aufgabe an Managed Service Provider delegiert, deren Tätigkeit unter anderem die unbedingt notwendige kontinuierliche Weiterentwicklung der Abwehrtechniken sowie die Suche nach besseren Tools und Möglichkeiten zum Schutz des geistigen Eigentums und der digitalen Ressourcen umfasst.

Die Unternehmen müssen genau nachvollziehen können, wie die Angreifer vorgehen. Dazu müssen sie eine Lifecycle-basierte Verteidigungsstrategie erarbeiten, die beschreibt, wie sie Angriffe erkennen, aufhalten und unterbrechen sowie Systeme wiederherstellen können.

Der vorliegende Bericht soll Sicherheitsteams dabei helfen, das bekannte Cyberangriff-Lebenszyklus-Modell, die sogenannte Cyber Kill Chain (CKC), sowie seine Erweiterung auf das gesamte Netzwerk zu verinnerlichen. Zudem geht der Bericht darauf ein, wie Panda Adaptive Defense Service den gesamten Lebenszyklus auf Endpoint-Ebene umfasst.

Die Cyber Kill Chain zeigt in gut verständlicher Weise auf, wie Unternehmen die Verteidigungsfähigkeit ihrer IT-Umgebung maßgeblich erhöhen können, indem sie Bedrohungen in jeder Phase des Angriffslebenszyklus erkennen und stoppen. Die Kill Chain vermittelt uns, dass wir die Kette „nur“ an irgendeinem Punkt des Prozesses durchbrechen müssen, um den Angriff zu vereiteln. Hingegen müssen die Kriminellen alle Phasen durchlaufen, um erfolgreich zu sein.

Denken Sie stets daran, dass wertvolle Vermögenswerte eines Unternehmens auf dessen Endpoints und Servern gespeichert werden. Daher wollen alle Angreifer bis zu den Endpoints vordringen, um Zugriff auf die wichtigen Assets der Unternehmen zu erlangen. Wenn Sie die Kriminellen am Endpoint aufhalten, wird ein erfolgreicher Cyberangriff wesentlich unwahrscheinlicher. Gleichzeitig wird das Durchbrechen der Kette erleichtert und die Effizienz sowie die Effektivität der Sicherheitsmaßnahmen werden erheblich erhöht.

Alle Angreifer wollen bis zu den Endpoints vordringen, um sich Zugang zu den wichtigen Assets des Unternehmens zu verschaffen. Wenn Sie die Kriminellen am Endpoint aufhalten, nimmt dadurch automatisch die Wahrscheinlichkeit eines erfolgreichen Cyberangriffs ab. Gleichzeitig wird das Durchbrechen der Kette erleichtert und die Effizienz sowie die Effektivität der Sicherheitsaktivitäten werden erheblich erhöht.

2.Was Sie über die Cyber Kill Chain wissen sollten

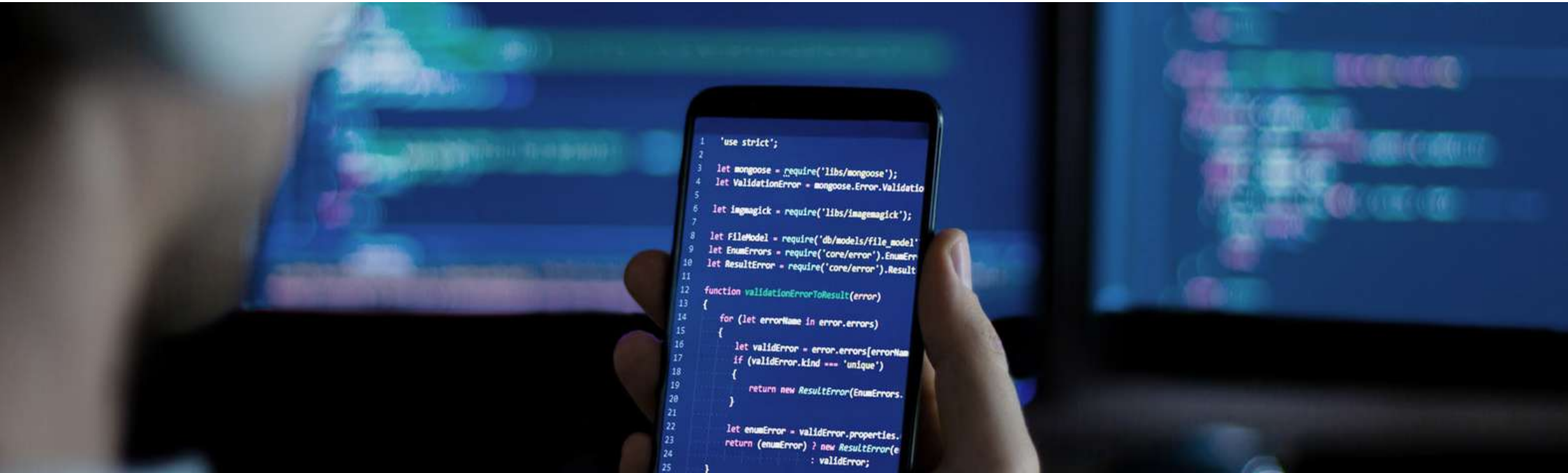
Das Konzept der Cyber Kill Chain wurde ursprünglich von Lockheed Martin im Rahmen seines Modells „Intelligence Driven Defense“[1] zur Ermittlung und Prävention von Cyberattacken veröffentlicht.

Das Modell klärt darüber auf, wie die Angreifer vorgehen müssen, um ihr Ziel zu erreichen: das Netzwerk ins Visier nehmen, Daten herausfiltern und den Fortbestand der Malware im Unternehmen sicherstellen. Das Modell zeigt, dass die Angriffskette unterbrochen wird, egal in welcher Phase wir die Angreifer stoppen. Angreifer müssen jedoch alle Phasen vollständig durchlaufen, um erfolgreich zu sein. Wir als Verteidiger müssen sie also nur an einem beliebigen Punkt blockieren.

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

Zudem bietet uns jedes Eindringen und jede Spur, die der Angriff am Endpoint hinterlässt, die Gelegenheit, mehr über unsere Gegner zu erfahren und ihre Hartnäckigkeit zu unserem Vorteil zu nutzen. Wenn wir die Motive und Handlungen der Angreifer besser nachvollziehen können, sind wir in der Lage, unsere Sicherheitsmaßnahmen effektiver zu gestalten.

Die Cyber Kill Chain zeigt die Phasen auf, die Cyberkriminelle bei ihren Angriffen durchlaufen müssen:



Externe Cyber Kill Chain

External Reconnaissance (Externe Erkundung)

Dieses Stadium kann als Phase der Zielauswahl und des Sammelns von Informationen über das Unternehmen, darunter branchentypische, marktspezifische und gesetzliche Anforderungen, genutzte Technologie, Social-Media-Aktivitäten und Mailinglisten, bezeichnet werden.

Der Angreifer sucht im Wesentlichen nach Antworten auf folgende Fragen: „Welche Angriffsmethode verspricht die größten Erfolgschancen?" und „Welche Methoden lassen sich in Bezug auf unseren Ressourceneinsatz am einfachsten ausführen?"

Weaponization and Packaging (Bewaffnung und Verpackung)

Dieser Schritt kann sich auf unterschiedlichste Weisen vollziehen: Ausnutzung von Webanwendungen, serienmäßige oder maßgeschneiderte Malware (zur wiederholten Anwendung heruntergeladen oder käuflich erworben), Schwachstellen in zusammengesetzten Dokumenten (PDF, Office und andere Dokumentformate) oder „Watering Hole Attacks".[2]

Dieses Vorgehen wird im Allgemeinen mit gelegenheitsbasierter oder sehr spezieller Intelligence in Bezug auf das Ziel vorbereitet.

Delivery (Übertragung)

Die Übertragung der Schadinhalte 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 (Ausnutzung)

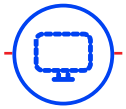
Nachdem die Schadinhalte an den Anwender, den Computer oder das Gerät übertragen wurde, manipulieren sie das Asset und verschaffen sich Zugang zur Umgebung.

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

Externe Cyber Kill Chain II

Installation

Bei der Installation findet oftmals eine aktive Kommunikation mit externen Akteuren statt. Dabei agiert die Malware normalerweise im Verborgenen, sodass der Angreifer sich dauerhaft an den Endpoints aufhalten kann, auf die er Zugriff hat. Er kann die Anwendungen dann vom Unternehmen unbemerkt kontrollieren.



Command and Control (Befehl und Steuerung)

In dieser Phase übernehmen Angreifer die Steuerung von Assets in ihrem Zielunternehmen. Dabei nutzen sie (häufig aus der Ferne) Steuerungsmethoden, die beispielsweise DNS, Internet Control Message Protocol (ICMP), Websites und soziale Netzwerke betreffen. Über diesen Kanal teilt der Angreifer dem von ihm gesteuerten Asset mit, was als Nächstes zu tun ist und welche Informationen gesammelt werden sollen.

Zu den entsprechenden Datensammelmethoden gehören Bildschirmaufnahmen, die Überwachung von Tastenanschlägen, das Knacken von Passwörtern, die Überwachung des Netzwerks auf Anmeldedaten sowie das Sammeln von sensiblen Inhalten und Dokumenten.

Häufig wird ein Staging-Host identifiziert, auf den alle internen Daten kopiert werden. Diese werden anschließend komprimiert und/oder verschlüsselt und für die Exfiltration vorbereitet.

Actions on Targets (Aktionen an den Zielpunkten)

In dieser abschließenden Phase geht es darum, wie der Angreifer Daten exfiltriert und/oder Schaden anrichtet. Dann werden Maßnahmen ergriffen, um weitere Ziele zu identifizieren, die Präsenz in einer Organisation auszuweiten und – besonders kritisch – Daten zu exfiltrieren.

Die Cyber Kill Chain (CKC) wird dann erneut in Gang gesetzt. Ein wichtiger Aspekt ist dabei, dass die CKC zyklisch abläuft und nicht linear. Wenn ein Angreifer in ein Netzwerk eindringt, startet er die Cyber Kill Chain erneut, um das Netzwerk weiter auszukundschaften und laterale Bewegungen auszuführen.

Ferner ist zu beachten, dass die Angreifer trotz gleicher Methodik für die einzelnen Schritte der internen Kill Chain andere Techniken anwenden, als wenn der Angriff von außerhalb gestartet wird.

Der Angreifer wird also zum Insider, zu einem Anwender mit Berechtigungen und fester Präsenz. 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.

3.Die erweiterte Version of the Cyber Kill Chain

Die Cyber Kill Chain ist ein zyklischer und nichtlinearer Prozess, bei dem der Angreifer ständige laterale Bewegungen innerhalb des Netzwerkes ausführt. Die innerhalb des Netzwerkes ablaufenden Phasen sind dieselben wie die, die für den ursprünglichen Angriff von außen genutzt wurden, auch wenn andere Techniken und Taktiken angewendet werden.

Die Kombination aus der externen und der internen Cyber Kill Chain wird in der Branche als „Erweiterte Cyber Kill Chain" bezeichnet. Dabei kommen weitere Schritte hinzu, die sich von den anderen nur dadurch unterscheiden, dass sie intern ausgeführt werden. So wird die externe Cyber Kill Chain durch die interne Cyber Kill Chain mit ihren eigenen Phasen ergänzt: Internal Reconnaissance, Internal Weaponization usw.

Jede Phase des Angriffs kann, sobald das Netzwerk des Opfers erreicht ist, von wenigen Minuten bis zu mehreren Monaten dauern, einschließlich einer Wartezeit.

Der Angreifer wartet dabei auf den optimalen Moment, 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.

Diese Phasen lassen sich nur schwer unterbrechen, da sie ohne direkte Verbindung zum Angreifer ausgeführt werden.

Deshalb ist es von besonderer Wichtigkeit, im Rahmen der Sicherheitsmaßnahmen an den Endpoints alle auf den Geräten laufenden Anwendungen permanent zu analysieren und zu überwachen. Auf diese Weise wird die Arbeit der Angreifer erheblich erschwert, sodass sich der Angriff für sie letztlich nicht rentiert.

Internal Reconnaissance (Interne Erkundung)

In dieser Phase haben die Angreifer Zugriff auf einen einzigen Endpoint eines Anwenders. Sie werden diesen nach lokalen Dateien, Netzwerkfreigaben und Browserverläufen durchsuchen sowie auf Wikis und SharePoint zugreifen. Die Angreifer wollen auf diese Weise herausfinden, wie dieser Rechner genutzt werden kann, um das Netzwerk kennenzulernen und an wertvolle Daten und Informationen heranzukommen.

Internal Exploitation (Interne Ausnutzung)

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.

Die Cyber Kill Chain

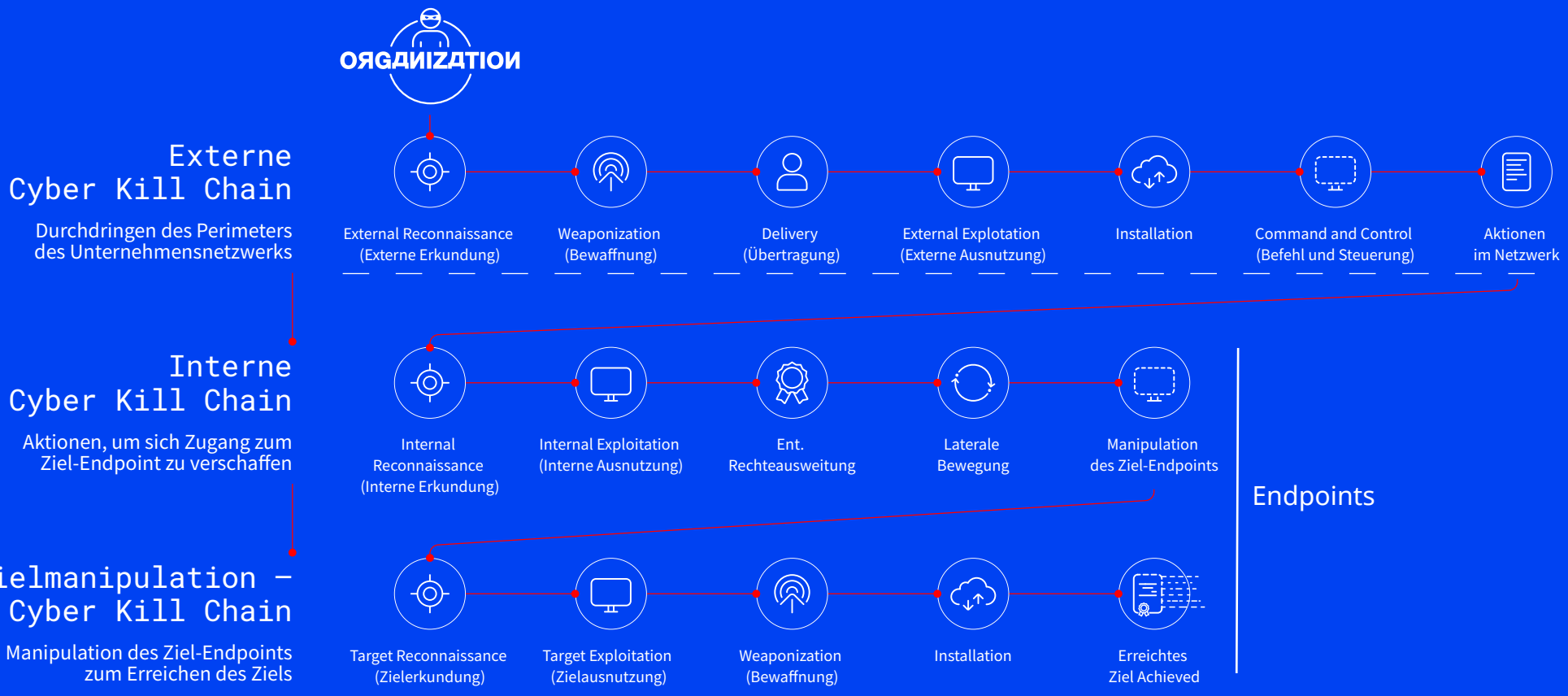


Abbildung 1: Die erweiterte Cyber Kill Chain. Aktionen des Angreifers, um sich Zugang zum Ziel-Endpoint zu verschaffen, und Endpoint-Manipulation zum Erreichen dieses Ziels.

4.Panda Adaptive Defense 360 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.

Das mehrschichtige Sicherheitskonzept von WatchGuard mit Panda Adaptive Defense 360 trägt dazu bei, die Cyber Kill Chain jederzeit zu durchbrechen und Angreifer mit leeren Händen dastehen zu lassen.

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, das Unternehmen besser gegen Angriffe zu rüsten. So lassen sich zwar nicht alle Angriffe verhindern, aber sie 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.

Wenn sich der Angriff auf das anvisierte Ziel wirtschaftlich nicht rentiert, werden die Angreifer auf andere Ziele im selben Unternehmen oder auf ähnliche Ziele in einem anderen Unternehmen ausweichen.

Die Sicherheitsstrategie von Unternehmen sollte zudem berücksichtigen, wie ein Angriff 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, die 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. So wird die Sicherheit des Unternehmens genau nach den Erfolgskriterien der Angreifer bemessen.

Dies wird jedoch durch eine Reihe von Faktoren erschwert. Anwendungen sind komplexer und stärker vernetzt als zuvor. Zudem sind sie anfällig, da der Großteil der Software nicht auf Grundlage angemessener Sicherheitsprinzipien entwickelt wird. Auch Mitarbeiter und Partner stellen weiterhin einen Hauptrisikovektor und ein Einfallstor für Angreifer dar, die mit Social Engineering arbeiten.

Die Lösung Panda Adaptive Defense 360 wirkt diesen Sicherheitsproblemen entgegen, indem sie auch die fortschrittlichsten Angriffstechniken in jeder Phase der erweiterten Cyber Kill Chain unterbindet, erkennt und darauf reagiert. Sie hilft Sicherheitsteams beim Erarbeiten einer Sicherheitsstrategie, die auf die erweiterte Cyber Kill Chain ausgerichtet ist – dank intelligenter Endpoint Detection and Response (EDR) ohne zusätzlichen Personalbedarf.

Die Grundpfeiler von Panda Adaptive Defense 360

Schutz vor bekannter Malware

Wenn Sie nur nach bekannten Bedrohungen suchen, können Sie Ihr Unternehmen nicht vor neuen Varianten oder anderen unbekannten Angriffsarten schützen. Doch durch eine Erweiterung um zusätzliche Schutzebenen können bekannte Bedrohungen präventiv gestoppt werden, wenn sie an den Endpoint übertragen werden. Panda Adaptive Defense 360 nutzt eine umfassende Sammlung an Reputationsservices, um Angreifer proaktiv zu blockieren, z. B. signaturbasierte Analyse, generische Signaturen, Heuristiken, Firewall, URL-Reputation, kontextuelle Erkennung, Schwachstellenmanagement, Anwendungskontrolle und weitere Funktionen, die das Risiko erheblich mindern können.

Darüber hinaus klassifiziert Panda Adaptive Defense 360 jede unbekannte Anwendung mithilfe von Schwarmintelligenz. **Schwarmintelligenz** ist diesem Fall das konsolidierte und immer weiter wachsende Wissens-Repository aller Anwendungen, Binärdateien und anderer Dateien, die interpretierten Code enthalten – vertrauenswürdigen wie bösartigen.

Dieses Repository in der Cloud wird kontinuierlich vom KI-System und von kompetenten Analysten befüllt und gleichzeitig vor jeder Ausführung von den Panda Security-Lösungen und -Diensten laufend abgefragt.

Erkennung fortschrittlicher und unbekannter Malware

Panda Adaptive Defense 360 erkennt und blockiert unbekannte Malware und gezielte Angriffe dank eines Sicherheitsmodells auf Basis von drei Prinzipien: ständige detaillierte Überwachung aller Anwendungen an den Endpoints, automatische Klassifizierung von Endpoint-Prozessen mithilfe von Big Data und Machine-Learning-Techniken in einer cloudbasierten Plattform sowie tiefgreifende Analyse nicht automatisch klassifizierter Anwendungen durch unsere Experten.

Diese drei Prinzipien bilden die Grundlage des **Zero-Trust Application Service**. Dieser Service klassifiziert Anwendungen als Malware oder legitim, sodass nur die vertrauenswürdigen Anwendungen an den jeweiligen Endpoints ausgeführt werden. Da der Service vollständig automatisiert ist, muss weder der Endanwender noch das Sicherheits- oder IT-Team aktiv werden oder eine Entscheidung treffen.

panda
a WatchGuard brand

Kontextuelle Verhaltenserkennung

Durch die kontinuierliche Überwachung der Aktivität am Endpoint kann der Agent als Sensor fungieren und die Cloud-Plattform nicht nur über die ausgeführten Dateien, sondern auch über deren Ausführungskontext zu informieren (Was ist unmittelbar vorher passiert? Welche Anwender versuchen, welchen Befehl oder welche Anwendung auszuführen? Welcher Netzwerkverkehr wird erzeugt? Auf welche Dateien wird zugegriffen? Welche Parameter usw.?).

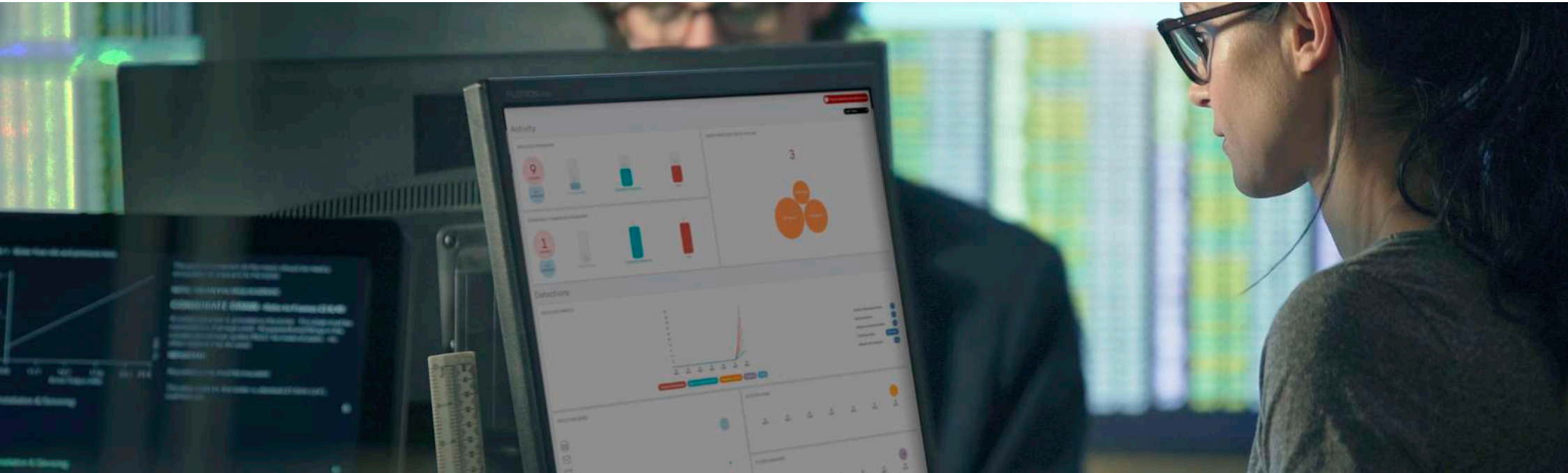
Dadurch ist es möglich, zunächst am Endpoint ungewöhnliche Verhaltensweisen oder verdächtige Aktivitäten zu erkennen und diese mit hoher Sicherheit und ohne falsch positive Ergebnisse als Angriffsindikatoren (Indicators of Attacks, IoAs) zu kategorisieren.

Dynamische Exploit-Erkennung

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 360 erkennt und blockiert 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 Angriffe dynamisch, indem sie alle auf den Geräten laufenden Prozesse permanent überwachen, Daten mittels Machine-Learning-Algorithmen 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.



Panda Adaptive Defense 360 in der Cyber Kill Chain

Vorbeugung und Schadensminderung

Ein Endpoint-Schutz der nächsten Generation muss Angreifer während der verschiedenen Phasen der Cyber Kill Chain präventiv abwehren und Angriffe schnell 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 Ausführung jeder unbekannten Anwendung blockiert, bis sie von unserem Machine-Learning-System und unserem Cybersicherheitsteam als vertrauenswürdig eingestuft wird; indem es jede verdächtige Aktivität im Zusammenhang mit den Techniken der Bedrohungsakteure blockiert; indem es die Malware unter Quarantäne stellt, einen kompromittierten Prozess abbricht oder gar das System vollständig herunterfährt, um den Schaden zu minimieren.

Abhilfe

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

Diese Veränderungen und Überbleibsel, die zurückgelassen werden, können Systemfehler und Instabilität verursachen oder sogar neuen Angriffen Tür und Tor öffnen. In den übrigen Fällen, in denen die Ausführung von Malware ermöglicht wird, stellt Panda Adaptive Defense 360 den Zustand wieder her, den die Endpoints vor der Malware-Infektion hatten.

Visualisierung

Angesichts der wechselnden Bedrohungslandschaft sowie der Häufigkeit, Raffinesse und Zielgerichtetheit der Angriffe 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 Unternehmen müssen einen Plan haben, wie sie gemeldete Sicherheitsverletzungen bearbeiten, wann diese gegebenenfalls den Strafverfolgungsbehörden gemeldet werden müssen und wie mit negativer Publicity und ähnlichen Begleiterscheinungen umzugehen ist.

Panda Adaptive Defense 360 bietet klare und frühzeitige Einblicke in schädliche Aktivitäten im gesamten Unternehmen. Aufgrund dieser Transparenz können Sicherheitsteams schnell das Ausmaß eines Angriffs beurteilen und entsprechende Maßnahmen ergreifen.

Reaktion auf Remote-Angriffe

Wenn Remote-Systeme das Ziel von Angreifern sind und kompromittiert werden, müssen IT- oder Sicherheitsteams schnell aktiv werden, um den Angriff nachzuvollziehen und Abhilfemaßnahmen zu ergreifen. Die Teams benötigen Transparenz in Bezug auf die Remote-Systeme und müssen auf diese zugreifen, da die Anwender nicht einfach ihren Laptop nehmen und damit zur IT-Abteilung gehen können.

Mit Panda Adaptive Defense können IT- und Sicherheitsteams dank detaillierter Endpoint-Transparenz die Vorfälle schnell untersuchen und neu auftretende Bedrohungen vollständig nachvollziehen. Darüber hinaus erhalten sie direkten Systemzugriff und können in kurzer Zeit eine zahlreiche Befehle ausführen, um Angreifer aufzuhalten und Probleme bei Remote-Hosts zu beheben, etwa indem Endpoints vom Netzwerk isoliert werden. Dabei wird die Kommunikation zu und von anderen Endpoints unterbunden, um die Ausbreitung des Angriffs zu verhindern. Eine weitere Maßnahme besteht darin, Prozesse durch Neustart des Endpoints zu beenden.

Aufgrund dieser Funktionen kann Panda Adaptive Defense 360 die Zeit für die Reaktion auf Angriffe – unabhängig vom Ort des Geschehens – erheblich verkürzen und schnell für die Fortführung des Betriebs sorgen.

Panda Adaptive Defense 360 in der Cyber Kill Chain

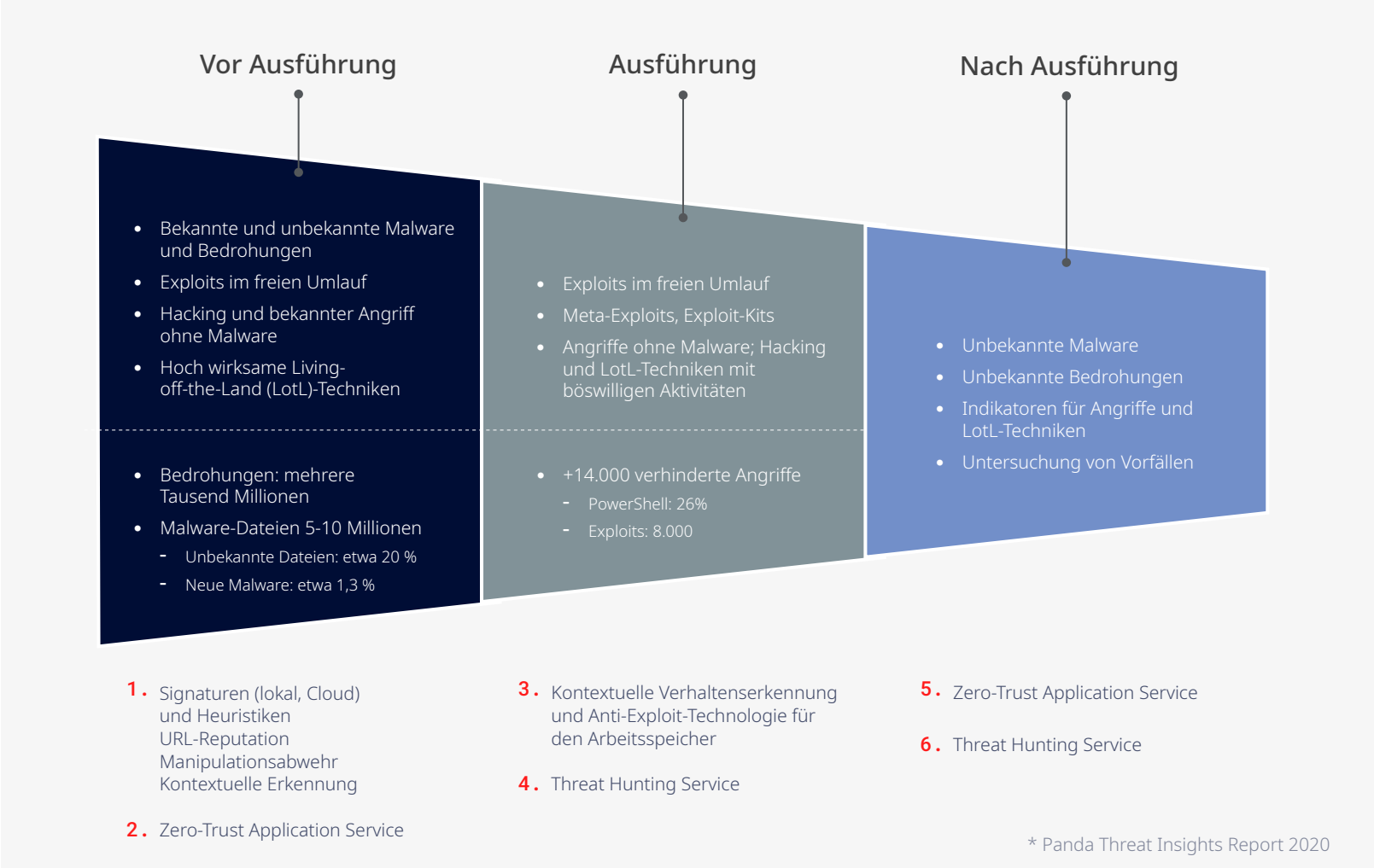


Abbildung 2: Die Grundpfeiler von Adaptive Defense 360 entlang der erweiterten Cyber Kill Chain.

5.Die Anatomie eines Ransomware-Angriffs und wie Panda Adaptive Defense 360 Ihr Unternehmen schützt

Abbildung 3 veranschaulicht, wie Panda Adaptive Defense 360 auf die einzelnen Kill-Chain-Phasen bei einem Ransomware-Angriff reagiert und laufende Angriffe verhindern und stoppen kann, bevor Schaden angerichtet wird.

Oftmals wendet der Angreifer einfache Techniken an, um sich Zugang zu einem beliebigen Ziel-Endpoint zu verschaffen – zumeist durch Social-Engineering-Methoden wie Phishing. Ein Anwender erhält eine E-Mail mit der Aufforderung, auf einen Link zu klicken oder eine bösartige Datei herunterzuladen.

SCHRITT 1

An dieser Stelle wird AD360 umgehend aktiv:

- Bösartige E-Mails werden mithilfe der E-Mail-Antispam-Technologie blockiert.
- Der Zugang zu bekannten bösartigen URLs wird durch den URL-Filter verhindert.

SCHRITT 2

Falls der Bedrohungsakteur nicht blockiert wird und der Endanwender auf die bösartige kompromittierte Website zugreift, können mehrere böswillige Aktionen erfolgen, etwa das Ausnutzen einer Browserschwachstelle oder das Herunterladen einer Microsoft Office-Datei mit einem bösartigen Skript.

In jedem Fall blockiert Adaptive Defense 360 den Angreifer mithilfe von Anti-Exploit-Technologien – entweder mit dem Anti-Exploit-Modul für den Arbeitsspeicher, das bekannte und unbekannte Exploits blockiert, oder durch die Makroprävention oder kontextbasierte Erkennung, die das Ausführen bösartiger Skripte verhindert.

SCHRITT 3

Hier gehen wir vom ungünstigsten Szenario aus, bei dem der Bedrohungsakteur in der Lage ist, Ransomware auf dem Gerät abzulegen. Panda Adaptive Defense 360 verhindert die Manipulation, indem die Lösung den Malware-Download blockiert. Dabei nimmt sie entweder einen Abgleich mit den lokalen generischen Signaturen vor und überprüft die Datei mit heuristischen Technologien oder sie fragt unsere Collective Intelligence in der Cloud ab.

Bei der Erkennung auf Basis generischer Signaturen geht es darum, Bedrohungen mithilfe einer einzigen Signatur zu erkennen und zu beseitigen. Die generische Erkennung hat ihren Ursprung darin, dass erfolgreiche Bedrohungen oft von anderen kopiert oder von den Originalautoren weiter perfektioniert werden. Dadurch kommt es zu einer Häufung von Ransomware-Varianten, die zwar alle unterschiedlich sind, aber zur selben Familie gehören. Die Anzahl der Varianten kann oftmals in die Hunderte, Tausende oder sogar Zehntausende gehen.

Die heuristische Überprüfung umfasst eine Reihe von Techniken zur Prüfung von Dateien auf der Grundlage Hunderter Dateieigenschaften. Auf diese Weise wird die Wahrscheinlichkeit ermittelt, dass ein Programm bösartige Aktionen vornimmt, wenn es auf dem Computer eines Anwenders ausgeführt wird. Dabei wird das Programm blockiert und entfernt, ehe es die Endpoints erreicht.

SCHRITT 4

Bisher haben wir uns mit Technologien befasst, die das Treiben der Bedrohungsakteure unterbinden, aber nicht garantieren können, dass am Endpoint keine bösartigen Anwendungen ausgeführt werden. Sie verringern jedoch deutlich den Arbeitsaufwand für den Zero-Trust Application Service, der die nächste Schutzebene in der Cyber Kill Chain darstellt. Nehmen wir also an, die Ransomware wird heruntergeladen und versucht, am Endpoint ausgeführt zu werden, um ihre bösartigen und schwer fassbaren Aktivitäten zu starten.

Zu diesem Zeitpunkt identifiziert der Zero-Trust Application Service die Binärdatei als unbekannt, verhindert ihre Ausführung, lädt sie in die Cloud hoch und klassifiziert die Payload automatisch mit einem komplexen, umfassenden Cluster von ML-Algorithmen. Dabei werden mehrere Hundert Attribute kombiniert, von denen viele daher stammen, dass die Sample in einer realen Umgebung in unserer Cloud-Infrastruktur gesprengt wurde.

Die Klassifizierung erfolgt zu 99,98 % in Echtzeit, da Ergebnisse nicht unbedingt überwacht werden müssen. Nur in Ausnahmefällen müssen unsere Experten für Cybersicherheit die Klassifizierung vervollständigen, da neue verdächtige Verhaltensweisen im Prozess hätten festgestellt werden können.

Die Abwehr der Cyber Kill Chain resultiert stets in einem echten Zero-Trust-Modell, bei dem keine bösartigen Anwendungen, Binärdateien oder Prozesse ausgeführt werden.

SCHRITT 5

Wenn Bedrohungsakteure in der Lage sind, ohne bösartige Anwendungen zu den Endpoints vorzudringen, nehmen andere Komponenten des mehrschichtigen Schutzes eine zentrale Position in der Cyber Kill Chain ein. Erlangt der Bedrohungsakteur beispielsweise die Kontrolle über einen Endpoint, setzt er sich dauerhaft dort fest und beginnt er damit, das Netzwerk mithilfe von Living-off-the-Land-Techniken auf neue Endpoint-Ziele abzusuchen, dann blockieren die kontextbasierten Erkennungstechnologien den Versuch des Missbrauchs von Systemtools wie PowerShell.

SCHRITT 6/7

Der wesentliche Faktor bei der effektiven Umsetzung des Zero-Trust-Modells besteht darin, dass jede Aktivität am Endpoint durch den Zero-Trust Application Service und den Threat Hunting Service in Echtzeit überwacht und ausgewertet wird. Dieser erkennt und untersucht verdächtige Aktivitäten und meldet oder blockiert bestätigte bösartige Aktivitäten an den Endpoints.

Erweitern Sie Ihre Transparenz und schützen Sie Ihr Unternehmen unabhängig vom physischen Standort. Testen Sie Panda Adaptive Defense 360

https://www.watchguard.com/wgrd-products/demos-free-trials

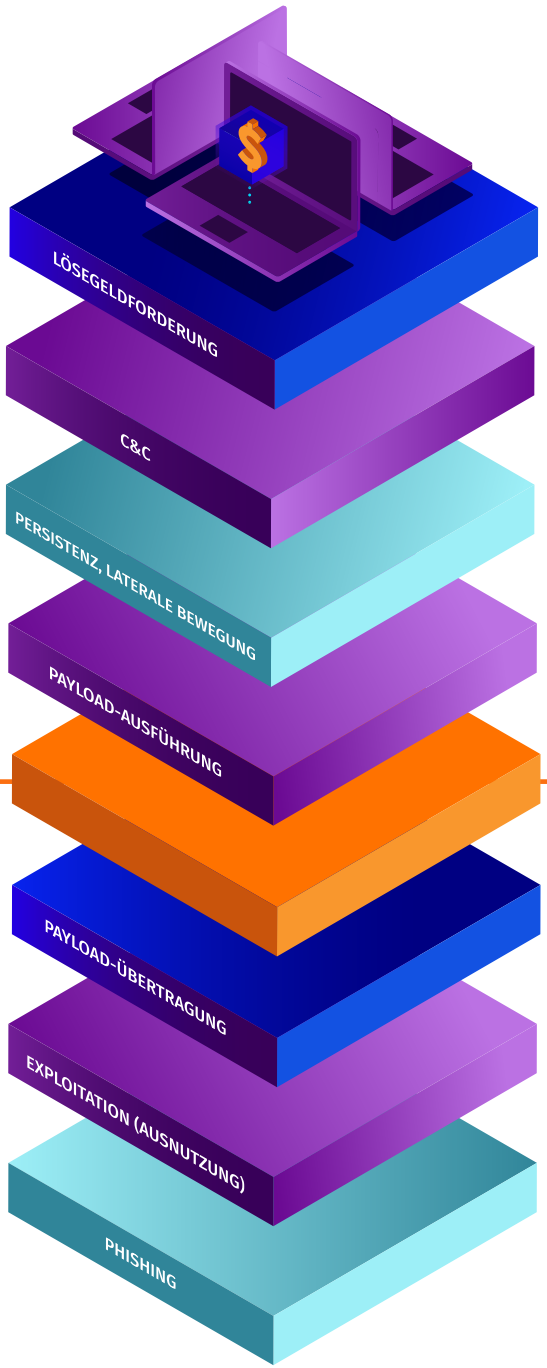
panda
a WatchGuard brand

Die Anatomie eines Ransomware-Angriffs

1. **Der Anwender erhält eine E-Mail mit der Aufforderung, auf einen Link zu klicken oder eine bösartige Datei herunterzuladen.**
2. Die Website nutzt eine **Browserschwachstelle aus** oder **lädt eine MS Office-Datei** mit einem bösartigen Skript herunter (Drive-by-Download-Angriff)
3. Nachdem der Anwender **geklickt hat, wird die Ransomware** an den Endpoint übertragen.
4. Die Ransomware wird am Endpoint ausgeführt und **startet ihre bösartigen und schwer fassbaren Aktivitäten.**

Es werden keine bösartigen Anwendungen, Binärdateien oder Prozesse ausgeführt.

5. Sobald der Bedrohungsakteur einen Endpoint unter Kontrolle hat, **erkundet er nach Netzwerk und sucht neue Ziele** (LotL-Techniken).
6. Die Ransomware versucht, über einen Command-and-Control-Server **an den Verschlüsselungsschlüssel zu kommen.**
7. Die Ransomware leitet den Prozess der Verschlüsselung von Dateien am Endpoint ein. **Die angezeigte Nachricht bestätigt das Auftreten von Ransomware** am Endpoint und fordert zur Lösegeldzahlung auf.



Panda Adaptive Defense 360 mit mehrschichtigem Schutz

1. Bösartige E-Mails werden mit **Antispam blockiert.**
   Der Zugang zu bekannten bösartigen URLs wird durch **URL Filtering verhindert.**
2. Die bekannte Ausnutzung von Browsern wird mittels **Anti-Exploit-Technologie blockiert.**
   Die unbekannte Ausnutzung von Browsern wird durch **Anti-Exploit-Technologie für den Arbeitsspeicher blockiert.**
   Die Skriptausführung mit durch **Makroerkennung oder kontextbasierte Erkennung blockiert.**
3. Bedrohungen werden nach dem Abgleich mit dem **cloudbasierten Repository blockiert.**
   Bekannte/Unbekannte **generalistische Signaturen und Heuristiken werden blockiert.**
4. **Zero-Trust Modell:** Jede von „außen“ (E-Mail, Internet, Netzwerk, Geräte) eingehende Binärdatei wird blockiert, bis sie klassifiziert wurde.
   Zero-Trust Application Service klassifiziert automatisch die Payload in der Cloud mit **ML und realer Umgebung.**

Es werden keine bösartigen Anwendungen, Binärdateien oder Prozesse ausgeführt.

5. Der Missbrauch von Systemtools (PowerShell) wird **durch kontextbasierte Erkennung blockiert.**
   Bösartiges Verhalten während der Ausführung wird **durch kontextuelle Verhaltenserkennung blockiert.**
6. **Der Zero-Trust Application Service** verhindert die Ausführung der Malware.
   In jedem Fall werden alle Prozesse vom **Zero-Trust Application Service kontinuierlich überwacht und neu klassifiziert.**
7. Die Telemetrie wird vom **Threat Hunting Service überwacht und analysiert.**

panda
a WatchGuard brand

6.Referenzen

- Cyber Kill Chain von Lockheed Martin: http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf
- Sean T. Mallon, Strategic Cybersecurity Leader & Executive Consultant, bei Black Hat 2016: Extended Cyber Kill Chain
- Mitre's Cybersecurity Threat-Based Defense
- Microsoft's Security Development Life Cycle
- Gartner Research, G00298058, Craig Lawson, 7. April 2016

[1] Eric M. Hutchins, Michael J. Cloppert, Rohan M. Amin, Ph.D.: Intelligence-driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains

[2] Watering Hole Attack: Eine spezielle Art von gezieltem Angriff, bei dem das Opfer zu einer bestimmten Gruppe gehört (Organisation, Branche oder Region). Bei diesem Angriff 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 bei diesen Angriffen eingesetzte Malware 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 Raubtieren in der Natur abgeleitet, die an Wasserlöchern auf eine Gelegenheit warten, ihre Beute anzugreifen. Auf Websites 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 Machine-Learning-Technologien analysiert werden. Diese sind darauf ausgerichtet, Versuche, vertrauenswürdige Anwendungen auszunutzen, zu erkennen. Das Ziel dieser neuen Technologie ist es, Angriffe auf Workstations und Server bereits in der Anfangsphase der Cyber Kill Chain zu stoppen. Angreifer werden in Schach gehalten und in solch einem Ausmaß am Zugriff auf das Gerät gehindert, dass sich der Angriff wirtschaftlich nicht mehr rentiert. Dies hält sie von weiteren Versuchen ab und führt somit zu einer höheren Erkennungsrate.

panda
a WatchGuard brand

VERTRIEB DEUTSCHLAND, ÖSTERREICH, SCHWEIZ +49 700 92229333 INTERNATIONALER VERTRIEB +1-206-613-0895 www.watchguard.com | pandasecurity.com

Weitere Informationen finden Sie auf unserer Website.