AUFDECKEN VON GEZIELTEN ANGRIFFEN MIT BROAD CONTEXT DETECTION™

F-SECURE WHITEPAPER

F-Secure

JEDES UNTERNEHMEN, DAS KEINE LÖSUNG ZUR ERKENNUNG VON SICHERHEITSVERSTÖSSEN BETREIBT (ODER KÜRZLICH KEINE UNTERSUCHUNG DAZU DURCHGEFÜHRT HAT), MUSS HEUTE UND IN ZUKUNFT DAVON AUSGEHEN, DASS ES SICH IN EINEM ZUSTAND NACH EINEM VERSTOSS BEFINDET.

F-Secure

EINFÜHRUNG

Im Bereich Cybersicherheit spielt sich derzeit ein Paradigmenwechsel ab. Gezielte Angriffe überlisten die traditionellen Präventions- und Erkennungsmechanismen der Unternehmen. Lösungen für den Endgeräteschutz sind nicht in der Lage, dateilose Angriffe zu erkennen, die durch das Verhalten und die Verwendung legitimer Betriebssystem-Tools charakterisiert sind und nicht durch bösartige Programme, die auf dem Computer installiert werden. Erkennungstechnologien bemerken zwar verdächtige Ereignisse, doch häufig gelingt es ihnen nicht, kritische Vorfälle aus dem Umgebungsrauschen herauszufiltern. Das führt zu einer überwältigenden Anzahl von Warnmeldungen, die niemals abgearbeitet werden können.

Laut einer EMA-Studie aus dem Jahr 2017 gaben 79 % der befragten Sicherheitsteams an, von einer hohen Anzahl von Bedrohungsmeldungen überwältigt zu sein. Das verwundert kaum: Eine Studie von Ovum ergab zum Beispiel, dass bei 37 % der Banken mehr als 200.000 Warnmeldungen pro Tag auflaufen und bei 61 % über 100.000. Das Ponemon Institute berichtet, dass fast die Hälfte aller Sicherheitswarnungen Falschmeldungen sind. Von den übrigen ist ein großer Teil wenig bedeutsam und leicht zu beheben.

Da sie nur die Möglichkeit haben, einem Bruchteil der Warnmeldungen auf den Grund zu gehen, sind überlastete Sicherheitsteams gezwungen, die meisten der täglich auflaufenden Warnmeldungen zu ignorieren. Das führt zu Frustration in den Teams. Die EMA fand heraus, dass 52 % des Betriebspersonals hohen Stress empfinden. 21 % gaben an, dass dieser durch „Personalmangel“ verursacht würde.[1] Die Kompetenzlücke im Bereich Cybersicherheit selbst ist gut dokumentiert. ESG und ISSA kamen 2017 zu dem Schluss, dass sich die Lage verschlechtere und 70 % aller Unternehmen betreffe.

Im Jahr 2018 nimmt Cybersicherheit im kollektiven Bewusstsein also zwar eine prominente Rolle ein,

doch die Unternehmen ringen nach wie vor mit Sicherheitslücken. Die durchschnittliche Dauer bis zum Entdecken einer Sicherheitslücke wird je nach Branche und Studie mit 100 Tagen oder mehr angegeben[3]. Unternehmen werden noch immer unvorbereitet von Sicherheitslücken getroffen, die ihre Netzwerke und die Daten ihrer Kunden offen legen.

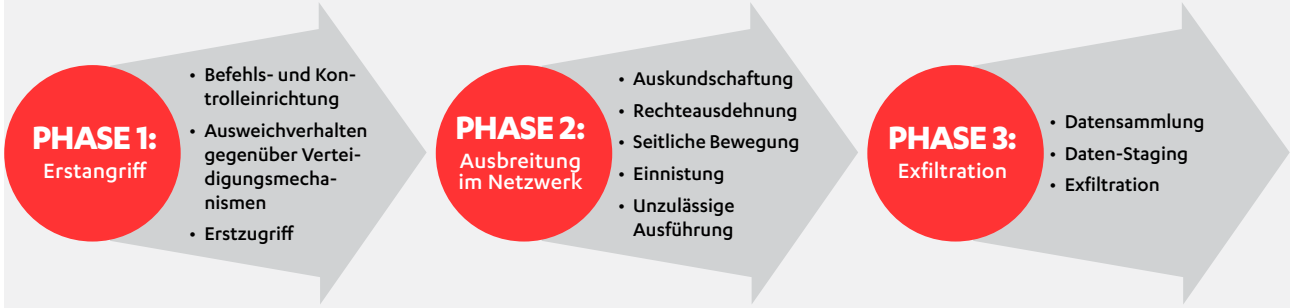
Die Angreifer setzen ihre Machenschaften verborgen in der Flut der Warnmeldungen fort.

KONTEXT IST ALLES

Wirklich alles. Im Leben und im Bereich der Cybersicherheit. Mit einem Schlüssel öffnet jemand das Schloss Ihrer Haustür. Dabei ist von entscheidender Bedeutung, ob die Person, die den Schlüssel umdreht, Ihr Ehepartner oder ein Einbrecher ist. Jemand verlässt ein Kaufhaus mit einer großen Tasche voller Einkäufe. Dabei ist von entscheidender Bedeutung, ob diese Person zuvor den Bezahlvorgang abgeschlossen hat oder nicht. Ein komplexer Powershell-Befehl wird auf dem Rechner eines Benutzers ausgeführt. Dabei ist von entscheidender Bedeutung, ob dieser es im Rahmen der Systemwartung oder von Microsoft Word ausgeführt wird.

Ablauf eines gezielten Angriffs am praktischen Fallbeispiel: Gothic Panda

Zur Erläuterung eines fortgeschrittenen und gezielten Cyberangriffs und Modell für das Verhalten von bösartigem Cyberverhalten dient hier das Beispiel der Gruppe für fortgeschrittene anhaltende Bedrohungen (Advanced Persistent Threat, APT), die in der Wissensdatenbank Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK™) von MITRE als Gothic Panda bekannt ist.[5] Die Angreifer sind in diesem Beispiel an der Exfiltration von Dokumenten und geistigem Eigentum oft aus der Industrie interessiert. Die Vorgehensweise von Gothic Panda kann in die drei nachfolgend dargestellten Hauptphasen unterteilt werden.



In der Phase des Erstangriffs streben die Angreifer eine erfolgreiche Codeausführung und Kontrollübernahme über ein System in der Zielumgebung an. Das Ziel der zweiten Phase, der Ausbreitung im Netzwerk, besteht darin, die gewünschten Systeme innerhalb der Zielumgebung zu identifizieren und sich auf diese auszudehnen, mit der Absicht, Zugangsdaten und Dokumente zur Exfiltration zu finden. In der letzten Phase geht es darum, die Daten zu sammeln, diese in der Zielumgebung in ein einfach zu übertragendes Paket zu komprimieren und dann die Exfiltration in anderem ausgehenden Netzwerkverkehr versteckt durchzuführen. Je nach defensiver Ausrichtung kann die Exfiltration viel lauter und auffälliger sein, als der Versuch, sich mit aktuellen Tools im Rauschen zu verstecken.

Aus der Erkennungsperspektive ist die wichtigste Phase natürlich die erste, bevor sich der Angreifer einnistet und seine Tätigkeiten auf die wertvollen Systeme innerhalb der Zielumgebung ausdehnt. Gut vorbereitete Unternehmen setzen eine Präventionsschicht wie Plattformen zum Endgeräteschutz ein, um gängige Malware-Bedrohungen wie Ransomware zu blockieren, was die Ausführung von bösartigem Code in der Zielumgebung in den meisten Fällen verhindert. Fortgeschrittene Angreifer sind jedoch in der Lage, durch unauffällige und langsame Angriffe unentdeckt zu bleiben und die Präventionsschicht schließlich zu umgehen. An diesem Punkt kommen Erkennung und Reaktion ins Spiel.

Kontextlosigkeit hingegen ist ein Mangel an fast allem, was man benötigt, um ein qualifiziertes Urteil zu fällen. Ohne Kontext sind einzelne isolierte Ereignisse bedeutungslos. Nur wenn die Punkte zwischen zusammenhängenden Einzelereignissen miteinander verbunden werden, kann ein vollständiges Bild entstehen.

Kontextlosigkeit ist die Hauptursache für die Übersättigung mit Warnmeldungen. Viele Systeme zur Erkennung von Eindringversuchen geben heute noch isolierte Warnmeldungen aus, die einzeln betrachtet zwar Anomalien darstellen, sich in Verbindung mit anderen Ereignissen jedoch als harmlos erweisen. Die unverhältnismäßig große Menge an Falschmeldungen führt zu einer noch stärkeren Überlastung von Sicherheitsteams und erhöht die Wahrscheinlichkeit, dass tatsächliche Vorfälle unerkannt bleiben.

MENSCH & MASCHINE

In Bezug auf die Denkweise müssen wir uns von der Vorstellung verabschieden, dass es bei der Cybersicherheit um Produkte und Dienstleistungen geht. Vielmehr geht es um Fertigkeiten. Erfahrung. Kompetenz. Unabhängig davon, welche Produkte und Lösungen Sie einsetzen, kommt es darauf an, eine hochkomplexe und in ständigem Wandel begriffene Umgebungs- und Bedrohungslandschaft proaktiv zu verwalten. Dazu sind entsprechende Fertigkeiten unentbehrlich. Leider sind diese Fertigkeiten Mangelware. Diese Problematik wird sich immer weiter zuspitzen, in dem Maße, wie digitale Möglichkeiten ein zusehends wichtiger Aspekt in allen Bereichen der Wertschöpfung werden.

Doch vielleicht ist es noch wichtiger, dass Fertigkeiten allein nicht genügen. So wie die Technologie unsere Möglichkeiten in allen Bereichen, von der Entwicklung bis hin zur produktiven Arbeit, potenziert hat, müssen wir Technologien entwickeln, mit denen wir unsere Fertigkeiten ausbauen und die uns dabei helfen, mit den Herausforderungen im Bereich Cybersicherheit Schritt zu halten. Wir müssen Technologien entwickeln, die lernen können, blitzschnell das zu tun, was menschliche Sicherheitsanalysten leisten – die einzelnen Punkte miteinander verbinden und Einzelereignisse zu einem stimmigen Gesamtbild zusammenführen, um ein qualifiziertes Urteil zu fällen.

Detektivisches Zusammensetzen der Fakten

Das Erkennen eines Gesamtkontexts lässt sich technisch nicht versierten Personen vereinfacht anhand einer Analogie zur realen Welt verdeutlichen. Stellen Sie sich ein Autowrack am Fuße eines steilen Abhangs vor. Gab es einen Unfall oder ein Verbrechen? War jemand in dem Auto? Diese wichtigen Fragen müssen beantwortet werden, um entscheiden zu können, wie auf eine solche Entdeckung reagiert werden muss.

Also werden forensische Ermittler zum Unfallort gerufen. Sie untersuchen die Unfallstelle, um die Abfolge der Ereignisse, die zum Absturz des Fahrzeugs führten, zu rekonstruieren. Sie untersuchen die Reifenspuren oberhalb des Abhangs, um festzustellen, ob der Wagen beschleunigt oder gebremst hat. Sie überprüfen den Tacho, um festzustellen, mit welcher Geschwindigkeit das Auto unterwegs war. Sie messen die Motortemperatur, um zu ermitteln, wie lange das Wrack schon dort ist. Sie nehmen einen Abgleich des Nummernschilds vor, um herauszufinden, auf wen das Fahrzeug registriert ist, und durchsuchen die Umgebung nach jeglichen Spuren menschlichen Ursprungs. Sie nehmen Ereignisse unter die Lupe, die in den vorangegangenen Wochen geschehen sind, wie z. B. ob der Fahrzeughalter verdächtige Anrufe erhalten hat oder sein Browserverlauf eine Suche auf einem Online-Kartendienst um die Klippe herum enthält. So werden Anomalien im Normalverhalten ausgeschlossen.

Für sich genommen scheint jeder dieser Faktoren, der Tacho, die Motortemperatur, die Ereignisse aus den Wochen vor dem Unfall usw., bedeutungslos zu sein. Wenn man sie jedoch im richtigen Kontext betrachtet, tritt eine Geschichte hervor, die den Ermittlern dabei hilft, den Unfallhergang zu rekonstruieren und festzustellen, ob ein Verbrechen begangen wurde.

BAHNBRECHENDER PARADIGMENWECHSEL

Aus der Abwehrperspektive ist dies ein bahnbrechender Paradigmenwechsel. Es kommt nicht in Frage, bestehende Lösungen zum Endgeräteschutz auszubauen und als neuartige Technologien zu vermarkten. Anbieter von Cybersicherheitslösungen müssen von Grund auf neue Lösungen entwickeln, die speziell auf die neue Ära und deren neue Probleme zugeschnitten sind.

Dies bringt eine Verschiebung von auf isolierte Vorfälle und punktuelle Erkennungen bezogene, binäre An-/Aus-Reaktionen hin zu Ereignisfluss- und kontextbasierten Erkennungen mit facettenreichen, risikobasierten Reaktionen mit sich.

Wir möchten Ihnen eine Vorstellung vom Ausmaß dieses Wandels geben: Unsere Backend-Systeme analysieren im Rahmen der traditionellen Lösung für den Endgeräteschutz tagtäglich über eine Million Proben und entscheiden darüber, ob diese Proben als bösartig einzustufen sind oder nicht. Das ist eine beeindruckende Zahl, die sich durch die Dutzenden Millionen von Endpoint-Clients erklärt, die bereits weltweit im Einsatz sind und diese Proben versenden.

In dieser neuen Ära, in der versucht wird, böswillige, versteckte Angriffsaktivitäten anhand von kleinen Einzelereignissen zu erkennen, die Angreifer bei der Ausführung ihrer Taktiken, Techniken und Verfahren auslösen, muss jedoch völlig anders vorgegangen werden. In einer einzigen mittelständischen Kundenumgebung mit 1.300 Endgeräten müssen wir täglich 70 Millionen Verhaltensereignisse analysieren.

Künstliche Intelligenz und maschinelles Lernen bilden dabei die einzige skalierbare Lösung, die dazu eingesetzt werden kann. Aber auch künstliche Intelligenz allein ist nicht die Antwort. Für sich genommen ist sie kaum mehr als eine viel gepriesene Maschine zur Erzeugung von Falschmeldungen. Vielmehr ist die perfekte Kombination aus Datenwissenschaften und menschlichen Cybersicherheitsexperten zur Lösung gefragt.

EINE LÖSUNG NIMMT GESTALT AN

Die Idee zu einer kontextabhängigen, durch Fachexperten optimierte Technologie entstand als Ergebnis von Gesprächen mit unseren Kunden. Wir haben sie gefragt, was ihnen in ihrem Unternehmen fehlt. Sie gaben an, dass sie über Systeme verfügen, mit denen sie die Standard-Malware stoppen, die 99,9 % aller Bedrohungen eines Unternehmens ausmachen. Was ihnen fehlte, war ein Tool, mit dem sie die verbleibenden 0,1 % der Bedrohungen stoppen können, die Unternehmen auf nicht herkömmliche Weisen infiltrieren.

Diese Bedrohungen richten den größten Schaden an. Dateilose Bedrohungen, die Ereignisse hervorrufen, die fast nicht von Ereignissen zu unterscheiden sind, die ein gewöhnlicher Benutzer hervorruft. Nur durch die Verbindung der einzelnen Punkte zwischen isolierten Ereignissen sind bösartige Muster erkennbar. Das Verbinden dieser Punkte ist die Tätigkeit, bei der der Sicherheitsanalyst in der Regel eingreifen muss.

Mit unserem 2016 eingeführten Rapid Detection & Response Service stehen die Dienste unserer hochkompetenten Cyber-Sicherheitsexperten für Unternehmen bereit. In unserem Rapid Detection & Response Center überwachen sie die Umgebungen unserer Kunden rund um die Uhr. Wenn eine Anomalie entdeckt wird, unterziehen unsere Experten diese einer sofortigen Analyse. Wenn sich dabei herausstellt, dass es sich um eine echte Bedrohung handelt, alarmieren sie den Kunden, und zwar innerhalb von 30 Minuten nach der Erkennung.

Es gibt nur ein Problem mit diesem Service: Die hochqualifizierten Experten sind nur begrenzt verfügbar. Wir haben erkannt, dass wir eine

Möglichkeit finden mussten, das Wissen und die Fertigkeiten der Experten aus unserem Rapid Detection Center Experten für jedes beliebige Unternehmen verfügbar zu machen. Also haben wir eine Technologie erarbeitet, die dem, was unsere menschlichen Experten leisten, so nahe kommt wie möglich: Dabei wird der Kontext einer Warnmeldung untersucht, um festzustellen, ob es sich um einen echten Vorfall handelt.

Das Ergebnis haben wir Broad Context Detection™ genannt.

INNOVATION VOM FEINSTEN

Missbrauch und bestimmungsgemäßen Gebrauch voneinander zu unterscheiden ist wie die Suche nach der Nadel im Heuhaufen. Es erfordert das Sammeln riesiger Mengen von Verhaltensereignissen. Broad Context Detection wurde entwickelt, um diese Flut von Ereignissen zu bezwingen und auf die wenigen wirklich bedeutsamen Ereignisse herunterzubrechen.

So erzeugt beispielsweise ein mittelgroßes Unternehmen mit 650 Sensoren in der Regel etwa 1 Milliarde Ereignisse pro Monat, von denen nur bei etwa zehn Erkennungen Eindämmungs- und Abhilfemaßnahmen erforderlich sind. Die Rolle von Broad Context Detection besteht darin, uns in die Lage zu versetzen, die wenigen Vorfälle, auf die es wirklich ankommt, in den Fokus zu nehmen. Dies geschieht, indem unzählige Ereignisse ausgewertet und Verdächtige gemeldet werden, woraufhin ähnliche Ereignisse miteinander verknüpft und als verwandte Ereignisse zu Gruppen klassifiziert werden, die mit einem Vorfall im Zusammenhang stehen. Broad Context Detection stellt die Ereignisse einer Gruppe schließlich auf einer Zeitachse dar und vermittelt so ein umfassendes Bild des eingetretenen Ereignisses.

Da beim Einsatz von Broad Context Detection

Broad Context Detection™ in Aktion

In einer Kundenumgebung mit 325 Knoten erfassten unsere Sensoren über einen Zeitraum von einem Monat rund 500 Millionen Ereignisse. Bei der Rohdatenanalyse durch unsere Backend-Systeme wurde diese Anzahl auf 225.000 verdächtige Ereignisse reduziert.

Diese verdächtigen Ereignisse wurden durch unsere Broad Context Detection™-Mechanismen weiter analysiert. Die Anzahl der Erkennungen ließ sich so auf nur 24 reduzieren. Schließlich wurden diese 24 Erkennungen von menschlichen Experten im Detail überprüft. Davon stellten sich wiederum nur 7 als echte Bedrohungen heraus.

Durch die Konzentration auf weniger und hochzuverlässige Erkennungen ist im Angriffsfall eine schnellere und effektivere Reaktion möglich.

der berechnete Risikowert mit jeder Erkennung je nach den Aktionen des Gegners steigt, werden die erfassten Verhaltensereignisse des ursprünglichen Angriffs aufgedeckt und der Verantwortliche für die Zielumgebung alarmiert. Der Gesamtkontext des Angriffs wird sofort auf der Zeitachse sichtbar und sämtliche betroffenen Hosts und relevanten Ereignisse sowie empfohlene Reaktionsmaßnahmen werden anzeigt.

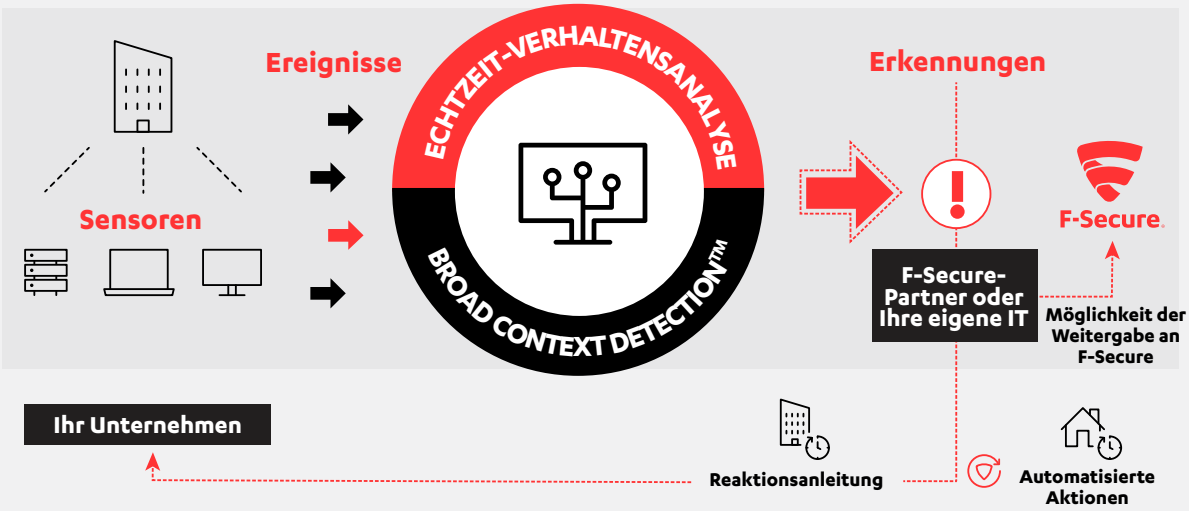
Dadurch kann der Angreifer frühzeitig aus dem Netzwerk isoliert werden, bevor er sich darin ausbreitet und Daten von Servern mit Kundendaten oder anderen persönliche Daten abgreift oder vertrauliche oder anderweitig sensible Geschäftsdokumente und geistiges Eigentum ausschleust.

FUNKTIONSWEISE

Wenn die Ereigniserkennung auf der Bereitstellung von Warnmeldungen basiert, verwundert das hohe Ausmaß der Falschmeldungen nicht. Die Broad Context Detection von F-Secure bringt die Erkennungstechnologie einen gewaltigen Schritt voran, indem sie aus der Menge der Warnmeldungen die tatsächlichen Vorfälle herausfiltert. Mithilfe von Kontext reduzieren wir eine lange Liste von Warnmeldungen zunächst auf eine kürzere Liste von Erkennungen und dann auf eine noch kürzere Liste von tatsächlichen Vorfällen. Diese dient als aussagekräftige Handlungsbasis für die Reaktion der Sicherheitsspezialisten.

Im ersten Schritt werden Einzelereignisse in Echtzeit an unsere Verhaltensanalysesysteme

F-Secure Rapid Detection & Response



1. Ressourcenschonende Sensoren überwachen Endpoint-Aktivitäten und übertragen Verhaltensereignisse in Echtzeit in unsere Cloud.
2. Die Verhaltensdaten zu Ereignissen werden in Echtzeit analysiert. Dabei werden sowohl die Prozesse als auch das Verhalten anderer Benutzer gemeldet und überwacht, die Ereignisse ausgelöst haben.
3. Broad Context Detection™-Mechanismen grenzen den Datenstrom weiter ein, setzen verwandte Ereignisse in einen Kontext zueinander, identifizieren tatsächliche Angriffe schnell und ordnen ihnen je nach Risikoeinstufung, Host-Kritikalität und vorherrschender Bedrohungslandschaft eine Priorität zu.
4. Warnmeldungen mit einer Visualisierung des Gesamtkontexts und beschreibenden Informationen zu dem Angriff erleichtern es dem F-Secure-Partner oder Ihrer eigenen IT, die Erkennung zu bestätigen, und bieten die Möglichkeit, besonders komplexe Untersuchungen an F-Secure zu weiterzugeben.
5. Nach einer bestätigten Erkennung führt die Lösung oder der Dienstanbieter Ihrer verwalteten Sicherheitslösung die IT- und Sicherheitsteams durch die notwendigen Schritte zur Eindämmung und Behebung der Bedrohung.

übertragen, die diese auf verdächtiges Verhalten hin untersucht und verdächtige Prozesse einer detaillierteren Überwachung zuführt. In dieser Überwachungsphase beziehen wir den Gesamtkontext ein. So können wir Ereignisse identifizieren, die bei einer isolierten Auswertung wahrscheinlich Falschmeldungen zur Folge hätten. In diesem Stadium können wir verdächtiges und feindliches Verhalten zuverlässig erkennen und akzeptables Verhalten ignorieren.

Die Flut von Warnmeldungen wird dann in einem weiteren Schritt aggregiert und es entsteht ein Bild des Kontexts, in dem mehrere verwandte Warnmeldungen gruppiert werden. Basierend auf dem umfassenderen Bild, das sich durch die Gruppierung von Warnmeldungen ergibt, lässt sich die Wahrscheinlichkeit von Falschmeldungen bei der Bewertung von tatsächlichen Erkennungen nahezu auf Null senken. Im letzten Schritt werden diese Erkennungen an eine Incident Detection Engine weitergeleitet, die tatsächliche Vorfälle bestätigt. Auch hier liegt die Falschmeldungsquote nahe Null.

Aus der so entstandenen viel übersichtlicheren, aber dennoch umfassenden Liste der Erkennungen wird eine Zeitleiste erstellt. Darauf werden die Erkennungen chronologisch angeordnet, um den Analysten ein Gesamtbild aller Umstände rund um den Vorfall zu verschaffen. Den Erkennungen werden auch abhängig vom Schweregrad, ihrer Risikoeinstufung, der Host-Kritikalität und der vorherrschenden Bedrohungslandschaft Prioritäten zugewiesen.

Mit diesem Ansatz erhalten die IT-Teams eine relativ kurze Liste von bestätigten Erkennungen, die jeweils mit unterschiedlichen Prioritätsstufen und empfohlenen Reaktionsmaßnahmen gekennzeichnet sind. So wissen die Teams nicht nur, worauf sie sich zuerst konzentrieren müssen, sondern sie wissen auch, wie sie reagieren müssen und können dies schnell und entschlossen tun.

ERKENNUNGEN UND VERHALTENSWEISEN

Die Broad Context Detection meldet Hinweise auf mögliche Sicherheitslücken, indem sie die Administratoren über Taktiken, Techniken und Verfahren informiert, die bei gezielten Angriffen eingesetzt werden. Dies kann beispielsweise die folgenden möglicherweise verdächtigen Aktionen umfassen:

- **Anormale Aktivität von Standardprogrammen**
- **Aufrufe an ausgeführte Prozesse aus nicht standardmäßigen ausführbaren Dateien**
- **Ausführen von nicht vorgesehenen Skripten**
- **Unerwartetes Ausführen von Systemwerkzeugen aus Standardprozessen**

Broad Context Detection meldet Taktiken, Techniken und Verfahren, die die folgenden Zwecke verfolgen:

- **Einnistung**
- **Rechteausdehnung**
- **Ausweichverhalten gegenüber Verteidigungsmechanismen**
- **Zugriff auf Anmeldeinformationen**

Mit Broad Context Detection™ wird das Ausmaß eines gezielten Angriffs leicht nachvollziehbar durch:

1. die kombinierte Echtzeitanalyse von Verhaltens- und Reputationsdaten sowie Big Data mit maschinellem Lernen
2. die Berücksichtigung von Risikoeinstufungen, Kritikalität der betroffenen Hosts und der vorherrschenden Bedrohungslandschaft, um einen umfassenden Einblick in einen Vorfall und dessen Schweregrad zu erhalten
3. die Reduzierung auf relevante Erkennungen mit aussagekräftiger Visualisierung für risikobasierte und vielschichtige Reaktionen

- **Auskundschaftung**
- **Seitliche Bewegung**
- **Unzulässige Ausführung**
- **Exfiltration**
- **Befehls- und Kontrollübernahme**

DAS MEISTE AUS MASCHINELLEM LERNEN HERAUSHOLEN

Der Einsatz von maschinellem Lernen und künstlicher Intelligenz, die fortlaufend durch menschliche Experten optimiert wird, bedeutet, dass unsere Systeme immer intelligenter werden. Im Gegensatz zu traditionellen Ansätzen, bei denen die Maschine lediglich darauf trainiert wird, wie bösartiges Verhalten aussieht, konzentriert sich unser Grundansatz auf die Modellierung von atypischem Verhalten. Das bedeutet, dass wir unseren Systemen beibringen, wie normales, „unbedenkliches" Verhalten aussieht, und dann alles darin einspeisen, was sich von dem unterscheidet, was wir erwarten. Damit können wir ein viel breiteres Spektrum an potenziell schädlichem Verhalten abdecken.

Dieser Ansatz bedeutet, dass wir uns nicht auf typische Angriffserkennungsmethoden beschränken, die auf Faktoren wie ungewöhnlich hohen Berechtigungen und schnellen Betriebsabläufen basieren. Kompetente Angreifer haben dies begriffen und auf minimale Berechtigungen und so genannte „unauffällige und langsame" Angriffe umgestellt. Sie gehen bei Angriffen also nach und nach vor und verteilen die einzelnen Angriffsphasen über einen längeren Zeitraum. Da solche Angriffe nicht den Mustern entsprechen, die zum Trainieren herkömmlicher Überwachungswerkzeuge eingesetzt wurden, gelangen sie nicht auf deren Schirm.

Der Vorteil des maschinellen Lernens besteht nun darin, dass wir die Maschinen so trainieren können, dass sie aus allem lernen, sogar aus ihren eigenen Fehlern (was beim Menschen nicht immer der Fall sein muss). Wenn die Maschine eine Warnmeldung als falsch identifiziert, lernt die Maschine, warum dies der Fall war, und berücksichtigt dies bei der nächsten Auswertung. So wird sichergestellt, dass derselbe Alarmtyp nicht mehr gemeldet wird. Dies ist einer der Gründe, warum unsere Falschmeldungsquote so niedrig ist.

Während Echtzeit-Erkennung die Basis unserer Lösung darstellt, ist es manchmal notwendig, etwas im Nachhinein zu erkennen. Dank maschinellem Lernen können wir neue Erkennungsregeln, die unsere Experten gerade erst festgelegt haben, leicht auf alte Daten anwenden, und Aktivitäten entdecken, die möglicherweise bei einem ersten Durchgang übersehen wurden.

Prävention macht den Angreifern das Leben schwerer

Auch wenn es fortgeschrittenen Angreifern ungeachtet aller Sicherheitsvorkehrungen gelingen sollte, in Ihr Netzwerk einzudringen, müssen Sie Ihnen nicht den roten Teppich ausrollen. Durch bessere Präventionsmaßnahmen erschweren Sie es diesen Angreifern, in Ihr Netzwerk einzudringen. Je höheren Aufwand sie betreiben müssen, desto höher fallen ihre Kosten aus. Dies dient als Abschreckungsmaßnahme.

Frühzeitige Prävention hilft Ihnen, die Erkennungs- und Reaktionsprozesse zu optimieren. Das ist aber nicht alles. Vielmehr besteht darin die kostengünstigste Methode zum Schutz Ihres Netzwerks. Je mehr Zeit ein Angriff in Anspruch nimmt, desto größere Kosten entstehen. Frühzeitige Prävention – und wenn diese fehlschlägt, schnellstmögliche Erkennung – hält die Kosten niedrig und Ihr Team bleibt dadurch effizient.

--

Unternehmen erkennen die Bedeutung von Prävention in der Regel erst dann, wenn es schon zu spät ist. Doch Schwachstellenmanagement mit Präventionsmaßnahmen ist im Zusammenspiel mit einer starken Erkennungs- und Reaktionsfähigkeit am besten dazu geeignet, Verstöße zu verhindern und Sicherheitslücken zu erkennen.

FAZIT

Bei der Cybersicherheit geht es um Fertigkeiten und Erfahrung. Aber das Dilemma des Verteidigers erinnert uns daran, dass wir genügend Ressourcen aufbieten müssen, um ständig auf der Hut zu sein, wohingegen die Gegner nach Belieben zuschlagen können. Angesichts des aktuellen Mangels an ausgebildeten Fachkräften befinden sich die Gegenspieler auf der Gewinnerseite.

Darüber hinaus reichen Fertigkeiten und Erfahrung allein nicht aus. Um dieses Fachwissen zur Überwachung eines ganzen Unternehmensnetzwerks nutzen und kleinste Hinweise auf einen Angriff erkennen zu können, ist Technologie nötig. Um dies präzise tun zu können, ohne unnötige Warnmeldungen zu produzieren, bedarf es überlegener Technologie. So können Zeit und Ressourcen für die Analyse tatsächlicher Vorfälle freigesetzt werden.

Broad Context Detection ist eine Kernfunktion der Rapid Detection & Response-Lösung von F-Secure. Sie bietet Unternehmen genau jene fortschrittlichen Funktionen, die diese zum Schutz vor gezielten Angriffen benötigen. Durch die leistungsstarken Möglichkeiten des maschinellen Lernens, das durch die Elite der Cybersicherheits-Fachleute ständig weiter optimiert wird, stellt Broad Context Detection sicher, dass die Lösungen von F-Secure nur wirklich relevante Vorfälle identifizieren. Durch diese ideale Kombination von Mensch und Maschine wird Cyber-Verteidigung auf Weltklasseniveau für jedes Unternehmen verfügbar.

Dank Broad Context Detection kann Ihr Unternehmen gezielte Angriffe erkennen, die bisher nicht erkennbar waren. Jetzt kämpfen und gewinnen.

Wir setzen auf unsere eigenen Lösungen

Unser System wird von unseren Experten ständig weiter optimiert und analysiert. Die Tatsache, dass es sich dabei um dieselbe Engine handelt, mit der wir unseren erstklassigen Dienst für verwaltete Erkennung und Reaktion bereitstellen, bedeutet, dass für unser System nicht einfach blind Daten auf der Grundlage von Lerndaten analysiert werden. Wir nutzen das System, um unseren Kunden Premiumservices anzubieten, und schleifen die Erkenntnisse aus diesen Kundenumgebungen dann ständig in die Lösung zurück. So können wir eine qualitativ hochwertigere und besser abgestimmte Lösung bieten als der Standardanbieter, der ausschließlich die Lösung herstellt. Wir selbst sind die Hauptanwender mehrerer Installationen, so dass das System auch aktiver Bestandteil unseres Tagesgeschäfts ist, mit dem wir uns vor gezielten Angriffen schützen.
Weitere Informationen zu den Premiumservice für verwaltete Erkennung und Reaktion von F-Secure finden Sie unter www.f-secure.de/RDS

[1] Enterprise Management Associates. A Day in the Life of a Security Pro (2017).

[2] American Banker. There are too many cybersecurity alerts (2017).

[3] Ponemon Institute for HPE. Cybersecurity Trend Report (2016).

[4] Information Systems Security Association International. ESG Survey Results (2017).

[5] The MITRE Corporation. Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK™) knowledge base (2018).

KRIMINELLEN KÖPFEN EINEN SCHRITT VORAUS

Wie erkennt man einen ausgeklügelten Angriff? Sie nutzen fortschrittlichste Technologien für Analyse und maschinelles Lernen. Doch das ist noch nicht alles. Sie müssen sich in den Angreifer hinein versetzen.

Die Sicherheitsexperten von F-Secure haben häufiger an europäischen Ermittlungsverfahren im Bereich Cyberkriminalität teilgenommen als jedes andere Unternehmen. Unsere Experten haben die neuesten Entwicklungen in der Cyber-Angriffslandschaft stets im Auge, damit sie über die jüngsten Bedrohungen im Bilde sind.

F-Secure®