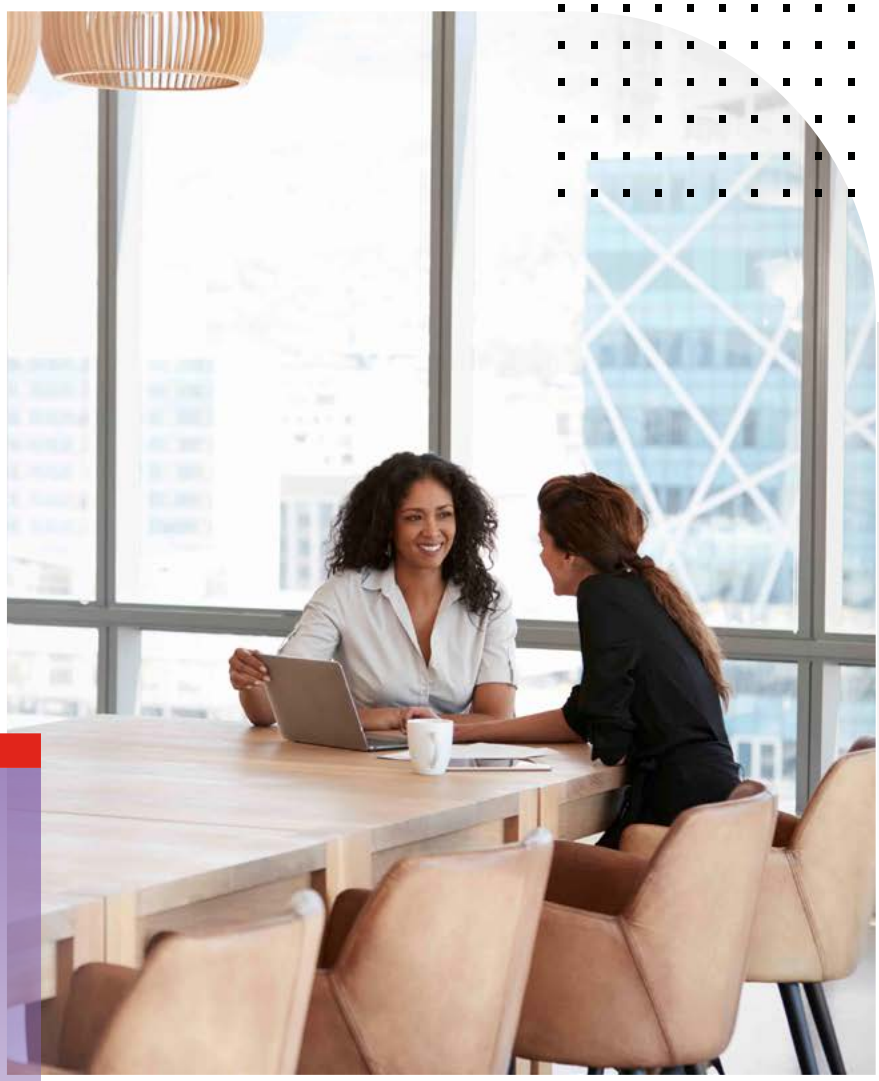
WHITEPAPER

Endpunkt-Sicherheit richtig bewerten

Welche Vorteile bringen MITRE Engenuity ATT&CK Evaluations?



Zusammenfassung

Die Entscheidung für die richtige Endpunkt-Security-Lösung ist komplex und sollte unbedingt auf objektiven, unabhängigen Informationen beruhen. Unternehmen können hierbei von MITRE Engenuity ATT&CK Evaluations profitieren, um die Wirksamkeit von Lösungen für die Endpunkt-Sicherheit richtig einzuschätzen. Diese Bewertungen eröffnen auch ein besseres Verständnis des aktuellen Sicherheitsprofils und zeigen Sicherheitslücken und mögliche Schwachstellen auf. Die Bewertungsergebnisse lassen sich zudem mit der umfassenden MITRE-Liste der Taktiken und Techniken vergleichen, die Cyber-Kriminelle bei Angriffen anwenden.

Bei der Endpunkt-Sicherheit dreht sich alles um die Risikominimierung. Security-Experten müssen deshalb vor der Evaluierung von Lösungen klären, ob gewisse Sicherheitsgrundlagen vorhanden sind, wie z. B. unternehmensweite Best Practices bei der Sicherheitshygiene, die die Angriffsfläche stark verringern können. Auch sollten Security-Experten eine Strategie zur Verbesserung des Sicherheitsprofils und der Transparenz haben. Sind diese Grundlagen gegeben, sind unabhängige Testergebnisse eine große Hilfe, um die beste Lösung für die eigenen Unternehmensanforderungen zu finden.

Die Endpunkt-Erkennung und -Reaktion (EDR) war die am häufigsten genannte Priorität auf die Frage an Unternehmen, welche Investitionsschwerpunkte bei der Endpunkt-Security in den nächsten 12 bis 18 Monaten geplant sind.[1]

Objektive Vergleiche von Security-Lösungen

Die sich ständig weiterentwickelnde Bedrohungslage hat heutzutage alles zu bieten: von „recycelten" Versionen bekannter Angriffe bis hin zu vollkommen unbekannten Cyber-Bedrohungen. Entscheidend ist, dass das Sicherheitsprofil des Unternehmens – und die einzelnen Sicherheitskontrollen, auf denen es basiert – stark sind und es auch bleiben. Allerdings ist die Bewertung von Cybersecurity-Produkten nicht immer einfach: Nicht nur die Ansätze unterscheiden sich oft, sondern auch die Begriffe, mit denen Sicherheitsfunktionen beschrieben werden. Unabhängige Tests, die solche Produkte bewerten, können Unternehmen beim Vergleich von „Äpfeln mit Äpfeln" helfen. Das schafft die Grundlage für besser informierte Entscheidungen und hilft, die richtige Lösung für die aktuelle Situation und das angestrebte Sicherheitsprofil zu finden. Leider lässt sich die Aussagekraft von Tests manchmal schwer einschätzen: Viele Tests beziehen sich auf die gesamte Security-Infrastruktur und liefern lediglich Ergebnisse wie „blockiert", „übersehen", „erkannt" oder „unerkannt", ohne die Testkriterien zu erwähnen.

MITRE ATT&CK Evaluations

Seit 2019 gelten die MITRE Evaluations als objektiver, detaillierter Test von Sicherheitslösungen. Bei diesen Tests werden reale Cyber-Angriffe und deren Techniken und Taktiken nachgebildet. Die Emulationspläne basieren auf öffentlichen Berichten über Cyber-Bedrohungen und werden auf Untergruppen von ATT&CK-Techniken angewendet. Damit wird das Verhalten von Angreifern simuliert, um objektive Fakten über die Leistung von Security-Lösungen zu erhalten. Die Ergebnisse zeigen nicht nur die technischen Möglichkeiten einer Lösung, um bestimmte Angriffe zu erkennen, sondern informieren auch über die Techniken und Taktiken vieler heutiger Cyber-Bedrohungen.

Die Bewertungen von MITRE Engenuity ATT&CK sind extrem aussagekräftig. Sie basieren auf dem MITRE ATT&CK Framework, einer Wissensdatenbank für Angriffstechniken. Die Vorgehensweisen bei Angriffen gegen bestimmte Betriebssysteme wie Windows werden genau aufgeschlüsselt und klassifiziert. Gegenüber älteren Testplattformen liegt der Schwerpunkt nicht auf den von Angreifern verwendeten Tools und der Malware, sondern darauf, wie mit Systemen während eines Angriffs interagiert wird.

Damit der Kontext stimmt, ordnet das ATT&CK Framework die Techniken verschiedenen Taktiken zu. Jede Technik umfasst relevante Informationen für Security-Teams, um den Kontext von Sicherheitsvorfällen oder Artefakten zu verstehen, die durch eine verwendete Technik erzeugt werden. Die Beziehung zwischen Taktiken und Technik lässt sich in der ATT&CK Matrix graphisch darstellen. Diese Matrix zeigt elf Einzeltechniken und bietet eine robuste, detaillierte Abbildung der Aktivität von möglichen Cyberangriffen. Jeder Bereich enthält mindestens zehn Taktiken, die alles abdecken – vom ersten Eindringen der Cyber-Kriminellen bis zu bestehenden CC-Verbindungen (Command-Control).

Im Jahr 2020 konzentrierten sich die ATT&CK Evaluations auf die Nachbildung von zwei Bedrohungsakteuren: der Carbanak-Gruppe, die auf Banken abzielt, und die auf finanziellen Gewinn ausgerichtete FIN7-Gruppe, die hauptsächlich den Einzelhandel, die Gastronomie und das Hotelgewerbe in den USA angreift und häufig Malware in Kassensysteme (PoS, Point of Sale) von Ladengeschäften einschleust. Beides sind ausgezeichnete Testfälle, weil sie:

- viel mit Scripting, Verschleierung und Malware-Versionen arbeiten, die sich schwer entdecken lassen und auf die Anwender eines Geräts, Systems oder Computers abzielen
- ein einzigartiges Spektrum an Dienstprogrammen verwenden – einschließlich hochkomplexer Malware und legitimer Management-Tools, die mit verschiedenen Plattformen interagieren können

2020 hat MITRE seine Bewertungen um Erkennungs- und Schutztests erweitert. Es ist nämlich nicht nur wichtig, ob eine Angriffsform rechtzeitig entdeckt und blockiert wird. Auch muss es möglich sein, nach der Blockierung der Taktik die Angriffsaktivitäten in späteren Phasen zu untersuchen.

Detection Test – der Erkennungstest

Bei Erkennungstests fließen 20 Testfälle in die Bewertung ein. Jeder Testfall umfasst mehrere Phasen. Für die Ergebnisse verwendet MITRE sechs Begriffe, die Aufschluss über das Abschneiden der Lösung bei jedem Test geben und auch über die Datenquelle für die Erkennung informieren:

- **Not Applicable** (Nicht anwendbar): Der Anbieter hat keinen Sensor im Testsystem implementiert.
- **None** (Keine Daten): Es liegen keine Daten darüber vor, ob die Sicherheitslösung das Testverhalten erkannt hat.
- **Telemetry** (Telemetrie): Das Verhalten wurde erkannt, aber minimal verarbeitet.
- **General** (Allgemein): Das Verhalten wurde verarbeitet und als Bedrohung gekennzeichnet, jedoch ohne Angaben, warum (Taktik) oder wie (Technik) der Angriff ausgeführt wurde.
- **Tactic** (Taktik): Das Verhalten wurde verarbeitet und als bösartig eingestuft. Außerdem werden die Taktik oder andere Informationen angegeben, warum der Cyberangriff so ausgeführt wurde.
- **Technique** (Technik): Das Verhalten wurde verarbeitet und als bösartig eingestuft. Außerdem werden die Technik oder andere Informationen angegeben, wie der Cyberangriff ausgeführt wurde.

Wird bei einem Erkennungstest eine Technik oder Taktik als nicht anwendbar angegeben, sollte man die Gründe dafür kennen. Das kann z. B. bedeuten, dass das Betriebssystem oder irgendeine andere fehlende Komponente die Implementierung verhindert. Es kann aber auch sein, dass die Sicherheitslösung die getesteten Verhaltensweisen nicht erkennen kann. Auch andere Gründe sind denkbar, die für Ihr Unternehmen vielleicht eine wichtige Rolle spielen.

In Fällen, in denen das getestete Verhalten auf womöglich legitime als auch bösartige Vorgänge hindeutet, muss das Ergebnis „None“ nicht unbedingt ein negatives Ergebnis sein. Das gilt insbesondere, wenn das Risiko, das Verhalten zuzulassen, ebenfalls mit „None“ angegeben wird. Das kann z. B. der Fall sein, wenn Cyber-Kriminelle noch nicht ihr Angriffsziel erreicht haben.

„Telemetry“ oder „General“ geben die erste Erkennungsstufe an, bei der das Verhalten identifiziert und von der Sicherheitslösung protokolliert wird. Allerdings gibt es nur begrenzte Informationen dazu, warum etwas erkannt wurde. Diese Stufe ist ausreichend für Unternehmen, denen die Zeit oder das Fachwissen fehlt, um das genaue Vorgehen von Cyber-Kriminellen und den geplanten Angriffsverlauf zu untersuchen. Erkennungsfunktionen, die die MITRE Evaluations mit „Tatic“ oder „Technique“ bewerten, sind besonders für erfahrene Security-Experten wertvoll, die die Aktivitäten der Angreifer genau nachvollziehen wollen.

Protection Test – der Schutztest

Bei Schutztests gibt es nur drei Begriffe:

- **Not applicable** (Nicht anwendbar): siehe oben unter „Erkennungstest“. Es kann aber auch bedeuten, dass der Testfall vor den restlichen Techniken blockiert wurde.
- **None** (Keine Nachweise): Nichts in der Sicherheitslösung deutet darauf hin, dass die Angriffstechnik blockiert oder sonst wie verhindert wurde.
- **Blocked** (Blockiert): Die Technik wurde blockiert und dem Benutzer wurde mitgeteilt, dass sie nicht erfolgreich war.

Obwohl es weniger Begriffe gibt, ist die Interpretation komplexer. Entscheidend ist, wann eine Bedrohung blockiert wurde, was je nach Testfall variieren kann. Die Bewertung gibt keinerlei Auskunft darüber, bei wie vielen erkannten „Bedrohungen" es sich um falsch-positive Ergebnisse handelt. Wird aber eine Bedrohung frühzeitig blockiert, kann dies mehr Fehlalarme bedeuten. Wird dagegen zu spät blockiert, kann das Unternehmen einem gewissen Risiko ausgesetzt werden – selbst wenn der Angriff nicht sein endgültiges Ziel erreicht. Wir haben für Sie ein paar Beispiele für jedes Szenario zusammengestellt:

Fortinet war an der MITRE 2020 Round der ATT&CK Evaluations beteiligt, die sich auf die Bedrohungsakteure Carbanak und FIN7 konzentrierte.

Angenommen, Test 1 wurde im ersten Schritt 1.a.1 blockiert. Das Ergebnis klingt erst einmal gut: Der Cyberangriff wurde zum frühestmöglichen Zeitpunkt gestoppt. Was aber, wenn in Wirklichkeit ein Benutzer daran gehindert wurde, etwas auszuführen? Dann wäre nämlich interessant, auf welcher Grundlage der Benutzer am Zugriff auf eine Datei gehindert wurde. Gab es einen starken Indikator für ein bösartiges Verhalten? Oder wurden zu strenge Richtlinien festgelegt? Anders verhält es sich im folgenden Fall: Nehmen wir an, dass die Blockierung am Ende von Schritt 2.b.5 erfolgte – beim Datenabgriff über einen CC-Kanal. In diesem Fall stoppte die Sicherheitslösung die beabsichtigte Datenverletzung, ermöglichte jedoch beim Schritt 2.b.1 das Kopieren der Daten per Fernzugriff (Remote File Copy). Und das bedeutet wiederum, dass der Angriff erfolgreich war.

In diesem speziellen Fall wäre Schritt 1.a.3 der sicherste Zeitpunkt, um den Angriff zu blockieren und um Fehlalarme sowie das Abgreifen der Daten zu verhindern. Dieser Schritt wird ausgeführt, wenn ein Skript die erste bösartige Datei-Manipulation versucht. Aber diese Informationen erhält man nur, wenn man jeden Schritt und jeden Teilschritt in jeder Phase verstanden hat. Erfolg oder Misserfolg hängen also auch von der „Kompromissbereitschaft" des Unternehmens ab, also der Frage: Wie stark schränken wir legitime Nutzeraktivitäten ein, um das Risiko eines erfolgreichen Cyber-Angriffs zu verringern?

Was Sie über die Bewertungsergebnisse wissen müssen

MITRE betont, dass es sich bei den Bewertungen nicht um eine Wettbewerbsanalyse handelt und es keine Punktzahlen, Rankings, Bewertungen oder „Gewinner" gibt. Stattdessen zeigt MITRE, was erkannt wurde und wie jeder Anbieter die Bedrohungserkennung nach den ATT&CK-Vorgaben angeht. Die Bewertungen können Unternehmen dabei helfen, Fragen zu beantworten wie:

- Erkennt eine Lösung bekannte Bedrohungen?
- Welche Daten liefert die Lösung für Analysten? Wie wird das aufbereitet?
- Können wir damit ein ausgewogenes Verhältnis zwischen einer aggressiven Erkennung bzw. einem guten Schutz und dem potenziellen Risiko einer Kompromittierung erreichen?

An den Bewertungen sehen Sie, welche Anbieter die größte Transparenz über Angriffstechniken bieten und welche Anbieter die von den Bedrohungen verwendeten Techniken am besten abwehren. Eine Bewertung kann Ihnen zeigen, welche Erkenntnisse Sie gewinnen können und wie oft eine Lösung aktualisiert wird, um Sie vor neuen Angriffstechniken zu schützen. Die Bewertungen können auch über andere Dinge Aufschluss geben, z. B. ob eine Lösung eine grafische Benutzeroberfläche (GUI) und einfache Optionen für weniger erfahrene Analysten bietet oder ob sie die Rohdaten liefert, die erfahrenere Analysten brauchen.

Folgende Fragen lassen sich jedoch nicht anhand der Bewertungen beantworten:

- Welche Auswirkungen hat eine Lösung auf Systeme und Benutzer?
- Wie hoch ist das Volumen der Warnmeldungen und der Umfang der notwendigen manuellen Recherchen und Untersuchungen?
- Wie passt die Lösung zu Ihrem allgemeinen Sicherheitsprofil? Ist sie eine Ergänzung oder besitzen Sie schon ein Produkt, das diese Sicherheitsfunktion bietet?
- Blockiert das System fälschlicherweise eine legitime Aktion?
- Wie lässt sich die Sicherheitslösung in Ihre anderen Security-Tools integrieren?
- Wie viel kostet die Lösung?

Um Antworten auf solche Fragen zu erhalten, sind zusätzliche Recherchen, Tests und die Berücksichtigung weiterer Unternehmensanforderungen nötig.

Was Sie aus den Bewertungen ziehen können

Der größte Wert von MITRE-Tests besteht darin, dass sie zeigen, wie gut eine Sicherheitslösung gegen Taktiken und Techniken funktioniert, die z. B. an Angriffsmustern erkennbar sind. Sie können so besser einschätzen, wie gut Sie eine Sicherheitslösung vor unbekannten Angriffen schützt. Die Bewertungen von MITRE basieren auf den Taktiken und Techniken, nicht auf den vorhandenen 1:1- oder 1:n-Bedrohungsinformationen oder -Modellen.

CISOs können die Ergebnisse der MITRE Engenuity ATT&CK Evaluations verwenden, um strukturelle Sicherheitslücken zu untersuchen. Keine Einzellösung kann jeden denkbaren Angriff oder jede existierende Technik erkennen. Aber Sie wissen so wenigstens, welche Sicherheitslösungen einen bestimmten Angriffstyp erkennen können. Am besten ist ein integrierter Ansatz, damit Unternehmen:

- Bedrohungen so früh wie möglich im Angriffsablauf erkennen und blockieren können
- ein ausgewogenes Verhältnis zwischen einer Blockierung nach einem Vorfall und einer frühzeitigen Blockierung erreichen
- herausfinden können, wie eine Lösung eine Bedrohung eindämmt. Blockiert sie bestimmte bösartige Aktionen in Echtzeit und entschärft sie sie durch Mikro-Eindämmung und Prozess-Isolierung? Oder verlässt sich das System auf die Netzwerk-Isolierung, damit sich Angreifer nicht ungehindert quer im Netzwerk bewegen können (laterale Bewegung)?
- auf umständliche oder manuelle Eindämmungsmaßnahmen wie das Beenden von Prozessen oder das Isolieren von Endpunkten nur in absolut notwendigen Situationen zurückgreifen müssen
- die Security Operations optimieren können

Behalten Sie die eigenen Ziele im Blick

Die Endpunkt-Security ist wichtiger denn je. Schnelle Angriffe wie Ransomware können in Minuten – wenn nicht Sekunden – Schaden anrichten. Die manuellen Reaktionen mit EDR-Tools der ersten Generation reichen dafür nicht mehr aus. Grundsätzlich sollte eine robuste Cyber-Security-Infrastruktur (einschließlich der Endpunkt-Sicherheit) das Gesamtrisiko reduzieren: Wirksame Sicherheitsrichtlinien und eine kontinuierliche Überwachung müssen vorhanden sein, um Angriffe zu entdecken, vorherzusagen, zu verhindern, zu erkennen, darauf zu reagieren und abzuwehren.

Entdeckung, Härtung und Prävention sind die Grundlagen jeder Sicherheitshygiene. Wenn Sie diese Basics richtig anwenden, können Sie Risiken drastisch reduzieren. Jeder CISO wird jedoch zustimmen, dass Prävention zwar wichtig, aber niemals hundertprozentig möglich ist.

Unternehmen müssen daher neben der Prävention auch in der Lage sein, Bedrohungen frühzeitig zu erkennen, schnell darauf zu reagieren und Angriffe einzudämmen. Entscheidend ist, dass Sie Sicherheitsverletzungen stoppen und schnell zu einem bekanntermaßen guten Zustand zurückkehren können. Letztendlich besteht das Ziel darin, Betriebsunterbrechungen minimal zu halten und die Ausfallsicherheit des Unternehmens sicherzustellen.

Mit den MITRE ATT&CK Evaluations können Unternehmen besser einschätzen, wie gut die Bedrohungserkennung einer Endpunkt-Sicherheitslösung funktioniert und welcher Schutz sich damit realisieren lässt. Bei der Auswahl der richtigen Endpunkt-Security für die eigenen Anforderungen sollten Unternehmen neben den MITRE-Ergebnissen aber noch Folgendes beherzigen:

- Praktizieren Sie eine gute Sicherheitshygiene mit Erkennung und Vorhersagen. So lässt sich die Angriffsfläche mit Transparenz und präventiven Kontrollen verringern, bis Patches verfügbar sind.
- Verbessern Sie die Korrektheit von Meldungen, um Teams nicht mit Fehlalarmen zu belasten, damit kritische Alerts in der Flut der Warnungen nicht übersehen werden.
- Legen Sie den Schwerpunkt auf die Abwehr und die Minimierung der Auswirkungen mit präzisen, automatisierten Reaktionen, um Risiken so gering wie möglich zu halten.
- Sorgen Sie für eine ständige Verfügbarkeit und Systemstabilität auch während eines Angriffs, insbesondere für Betriebstechnik (OT) und Management-Systeme.
- Nutzen Sie das volle Potenzial Ihrer Technologien – kein Tool installiert und wartet sich von selbst.

Fazit

MITRE ATT&CK Evaluations bieten mehr als eine simple Einschätzung der Wirksamkeit einer Sicherheitslösung. Ihr Schwerpunkt liegt darauf, wie eine Lösung funktioniert. Der große Vorteil dieses Ansatzes ist, dass Sie so nicht die „Katze im Sack" kaufen, sondern vorher wissen, was sie von den Sicherheitsfunktionen erwarten können. Und gemeinsam mit anderen Bewertungen erhalten Sie noch aussagekräftigere Einblicke als mit dem getesteten Sample-Set. MITRE ATT&CK Evaluations sind eine hervorragende Ressource, um die Suche nach der richtigen Cybersecurity-Lösung für Ihre speziellen Schwachstellen zu erleichtern und zugleich die Auswirkungen auf Menschen, Prozesse und Systeme zu berücksichtigen. Die Bewertungen können Ihnen ebenfalls dabei helfen, die Eignung einer Lösung für Ihre gesamte Security-Infrastruktur und Ihr Sicherheitsprofil zu bestimmen.

Allerdings sollte keine Sicherheitslösung im „luftleeren Raum" existieren: Bestimmte Angriffsformen lassen sich nicht allein am Endpunkt erkennen und manchmal kann bösartiges Verhalten von mehreren Lösungen erkannt werden. Obwohl doppelte Sicherheitsfunktionen besser als gar kein Schutz sind, kann eine mangelnde Integration auch neue Probleme mit sich bringen.

[1] David Gruber: „ESG Master Survey Results: Trends in Endpoint Security". ESG, 5. März 2020.

FORTINET

www.fortinet.com/de

12. August 2021, 13:41 Uhr
C:\Users\klaudia.chatowska\Desktop\WP_AccessYourEndpointSecurity\WP_AccessYourEndpointSecurity\A4\wp-FA-assess-your-endoint-security-4202021-A4-sources-files\wp-FA-assess-your-endoint-security-4202021-A4
968201-0-1-DE