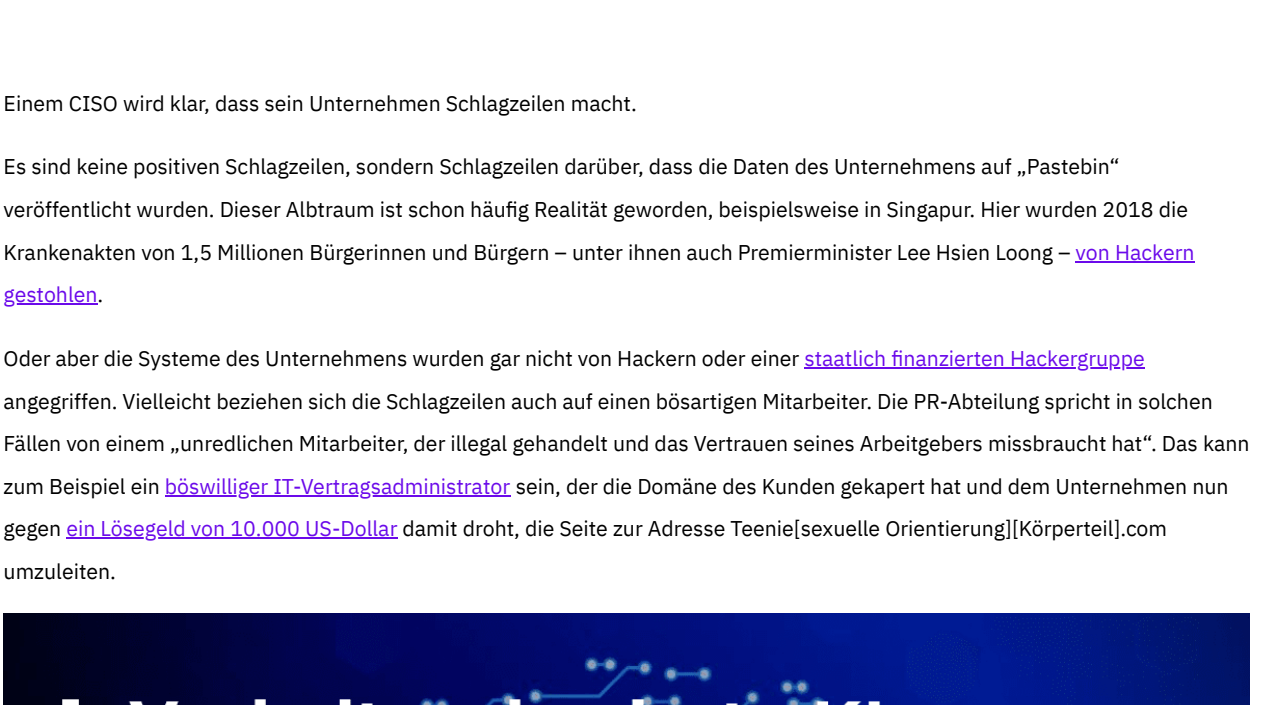

Verhaltensbasierte KI: Der uneingeschränkte Schutzansatz für Unternehmen

August 3, 2020
by Lisa Vaas

Einem CISO wird klar, dass sein Unternehmen Schlagzeilen macht.

Es sind keine positiven Schlagzeilen, sondern Schlagzeilen darüber, dass die Daten des Unternehmens auf „Pastebin" veröffentlicht wurden. Dieser Albtraum ist schon häufig Realität geworden, beispielsweise in Singapur. Hier wurden 2018 die Krankenakten von 1,5 Millionen Bürgerinnen und Bürgern – unter ihnen auch Premierminister Lee Hsien Loong – von Hackern gestohlen.

Oder aber die Systeme des Unternehmens wurden gar nicht von Hackern oder einer staatlich finanzierten Hackergruppe angegriffen. Vielleicht beziehen sich die Schlagzeilen auch auf einen bösartigen Mitarbeiter. Die PR-Abteilung spricht in solchen Fällen von einem „unredlichen Mitarbeiter, der illegal gehandelt und das Vertrauen seines Arbeitgebers missbraucht hat". Das kann zum Beispiel ein böswilliger IT-Vertragsadministrator sein, der die Domäne des Kunden gekapert hat und dem Unternehmen nun gegen ein Lösegeld von 10.000 US-Dollar damit droht, die Seite zur Adresse Teenie[sexuelle Orientierung][Körperteil].com umzuleiten.

Unternehmen können auf verschiedenste Weise in die Negativ-Schlagzeilen und in diese Art von Cybersicherheitsmisere geraten. Meist ist auch die Polizei involviert – entweder das Unternehmen erstattet Anzeige oder es wird von der Polizei auf den Zwischenfall aufmerksam gemacht. Für die genauen Details interessieren sich auch Journalisten und die Staatsanwaltschaft. Viel wichtiger für das Sicherheitskontrollzentrum (SOC) ist jedoch der Ablauf der Angriffe: Wie sind sie passiert, wer ist dafür verantwortlich und wie lässt sich der Angriff abwehren (sofern noch nicht geschehen)? Diese Geschichten bleiben oft genug unbekannt, weil sie in der Datenflut so schwer erkennbar sind. Schließlich umfasst diese sowohl verdächtige als auch ganz banale Systemaktivitäten, die das Team zu aufwändigen Untersuchungen veranlassen und sich am Ende als harmlose Systemanomalien herausstellen.

Diese komplizierten Storylines beginnen häufig auf den Endpunkten in einem Unternehmenssystem. Eventuell findet ein Mitarbeiter ein USB-Gerät auf dem Parkplatz und verbindet es aus reiner Neugier mit seinem Endgerät. Oder eine Mitarbeiterin öffnet auf ihrem Endgerät einen schädlichen PDF-Anhang, den sie per E-Mail bekommen hat.

Um einen genauen Überblick zu erhalten, ist es also sinnvoll, die für Angriffe typischen Endpunkte im Blick zu behalten. Bei einer Umfrage des SANS Institute im Jahr 2018 gaben 42 % der Befragten an, dass es bei ihnen zu mindestens einer Endpunktausnutzung gekommen ist, die zu Offenlegung, Exfiltration oder geschäftlichen Störungen führte. Hinzu kommt, dass die Verschlüsselung auf Endpunkten unauffällig im Hintergrund erfolgt, da hier die Netzwerk- und Prozessaktivitäten verfügbar bleiben und selbst externe Geräteüberwachung möglich ist. So lässt sich zum Beispiel feststellen, wer das USB-Gerät angeschlossen hat – und auch wann und wo.

Zu viele Datenpunkte, nicht genug Antworten

Wir haben durchaus schon Lösungen zur Endpunktüberwachung, die uns Antworten liefern können. Angriffe sind für uns heute sehr viel transparenter als zu EPP-Zeiten (Endpoint Protection Platform). Diese Produkte stützten sich auf Virussignaturen, waren aber für speicherbasierte Malware, laterale Bewegungen, dateilose Malware oder Zero-Day-Angriffe gänzlich blind.

Und hier liegt das Problem: EPP bietet durchaus Schutz für Endpunkte, bietet Unternehmen jedoch keinen Einblick in die Bedrohungen. EDR-Tools (Endpoint Detection and Response) der ersten Generation waren ein Nebenprodukt des von EPPs nicht bedienten Bedarfs nach Transparenz. Diese EDR-Generation – nennen wir sie passive EDR – bietet uns zwar Daten, jedoch ohne Kontext. Wir haben die Puzzleteile, aber kein Gesamtbild, das uns hilft, sie zusammenzusetzen.

Betrachten wir zum Beispiel integrierte, passive Endpunktüberwachung und nehmen wir an, dass Windows-Ereignisprotokolle eine USB-Kompromittierung erkannt haben, die zu einem PowerShell-Aufruf über eine virtuelle Tastatur führte. Sie erfahren, dass der Angriff hochentwickelte Techniken verwendet (etwa das Protokoll gelöscht) hat oder dass eine Backdoor installiert wurde, um Persistenz zu erzielen. Es wurden Login-Daten gestohlen, die für eine erfolgreiche Anmeldung genutzt wurden – und dann, *Überraschung!*, klappte die Anmeldung auf einmal nicht mehr. Stattdessen wurden Berechtigungen eskaliert, Protokolle gelöscht, ein lokaler Benutzer angelegt, der dann in eine Admin-Gruppe aufgenommen wurde, und so weiter. Viel Spaß beim Lösen des Problems.

Was als Demo vielleicht ganz nett aussah, bewährt sich im Alltag nicht unbedingt. Wer wird daraus schlau – außer vielleicht ein paar wenigen erfahrenen, sachkundigen Analysten, von denen es viel zu wenige gibt. Außerdem müssen sie ja irgendwann auch mal schlafen. Wenn also um Mitternacht ein Angriff stattfindet, freuen sich die Angreifer über die längere Verweilzeit, bis die Analysten wieder an die Arbeit gehen und alle Fragen zum Was, Wo, Wie und Wer beantworten.

CISOs wollen nicht unbedingt jeden einzelnen, zusammenhanglosen Datenfetzen zum Angriff erwischen. Es ist eher wie eine Partie Cluedo: War es Oberst von Gatow im Salon, ein Auftragnehmer mit einem USB-Laufwerk oder die staatlich unterstützte Hackergruppe? Wurde die Bedrohung schon abgewehrt, und wenn ja, wie lange war sie aktiv? Wer von den viel zu wenigen Analysten im SOC analysiert gerade diesen Daten-Tsunami, der aus der passiven EDR herausströmt?

Was ist verhaltensbasierte KI und wie kann sie helfen?

Was passiert nach einem Angriff? Die Geschichte kann zwei unterschiedliche Wege nehmen. Den ersten, sehr problematischen kennen Sie wahrscheinlich: Sicherheitsanalysten müssen sich durch alle Warnmeldungen und Anomalien wühlen, die die passive EDR ausgibt. Diese Untersuchungen erfordern ein knappes Gut – Zeit und Knowhow. Es ist bekanntlich schwer, Personal zu finden, zu schulen und zu halten, das die nötigen Kenntnisse für den Betrieb von Sicherheitsplattformen hat und in der Lage ist, die Spreu vom Weizen zu trennen, also die echten Exploits von den zufälligen Fehlern.

Doch die Geschichte kann auch eine andere Wendung nehmen und beinhaltet dann Storylines – durch die Kontextualisierung aller unterschiedlichen Datenpunkte in einem kurzgefassten Bericht. SentinelOne nennt das dann ActiveEDR. Durch dieses verhaltensbasierte KI-Modell sind Unternehmen nicht mehr ausschließlich auf die schwer aufzutreibenden Analystenfähigkeiten angewiesen. Es ist rund um die Uhr verfügbar, zeichnet durchgängig alles auf und liefert Kontextinformationen dazu, was auf jedem mit Ihrem Netzwerk verbundenen Gerät passiert.

Das verhaltensbasierte KI-Modul von SentinelOne erstellt das, was SentinelOne auch „Storyline" bezeichnet: eine Reihe von Spuren, über die Unternehmen Zwischenfälle zurückverfolgen und herausfinden können, wer für einen Kompromittierungsindikator (Indicator of Compromise, IOC) verantwortlich ist. Das ist zwar EDR, aber nicht die passive EDR, die Sie vielleicht bereits kennen. Die traditionelle EDR sucht erst nach einer isolierten Aktivität und versucht dann, sie mit einer anderen Aktivität und noch einer und noch einer zu korrelieren. Das ist der langwierige, nachträgliche Versuch, das große Ganze zu verstehen, für den zudem umfangreiche Fachkenntnisse erforderlich sind.

Bei SentinelOne ActiveEDR *übernimmt die Maschine die Arbeit* der Analysten. Alle Aktivitäten auf einem Gerät werden verfolgt sowie kontextualisiert und schädliche Handlungen in Echtzeit identifiziert. Erforderliche Reaktionen laufen dann automatisch ab. Wenn die Analysten eingreifen wollen oder müssen, vereinfacht ActiveEDR das Threat Hunting mit umfassenden Suchvorgängen von einem einzigen IOC ausgehend.

Im Gegensatz zu anderen EDR-Lösungen benötigt ActiveEDR keine Cloud-Konnektivität für eine Erkennung, wodurch die Verweildauer von Bedrohungen effektiv verkürzt wird. Die KI-Agenten auf den einzelnen Geräten benötigen keine Cloud-Verbindung, um Entscheidungen zu treffen. Sie zeichnet durchgängig die Abläufe der Ereignisse auf dem Endgerät auf. Wenn sie schädliches Verhalten entdecken, können sie nicht nur schädliche Dateien und Prozesse entfernen, sondern die komplette Storyline herunterfahren – und sogar automatisch rückgängig machen.

Warum ist ActiveEDR besser darin, dateibasierte und dateilose Angriffe aufzuhalten?

Raffinierte Angreifer haben eine Möglichkeit gefunden, sich ohne Dateien und Spuren zu bewegen. Sie verwenden dafür dateilose speicherinterne Malware, die selbst ausgereiften Sicherheitslösungen entgeht. Da ActiveEDR jedoch alles nachverfolgt, können Sie Angreifer erkennen, die vielleicht schon Anmeldedaten für Ihre Umgebung haben und nach dem LotL-Prinzip (Live off the Land) vorgehen: Dieser Begriff beschreibt dateilose Angriffe ohne Malware, die die systemeigenen, komplett seriösen Tools verwenden, um ihre schmutzige Arbeit zu erledigen. Dadurch fügen sie sich in das Netzwerk ein und verstecken sich zwischen den legitimen Prozessen, um den Exploit im Verborgenen durchzuführen.

Verhaltensbasierte KI – Ein Szenario aus der Praxis

Dieses reale Szenario zeigt die Funktionsweise: Die Polizei meldet sich bei Ihnen und teilt Ihnen mit, dass Ihre Anmeldedaten über Pastebin offengelegt wurden. Sie wollen wissen, wie es dazu gekommen ist. Also sehen Sie im Deep Visibility Threat Hunting-Modul nach. Deep Visibility ist ein Output der Storylines von SentinelOne. Es beschleunigt das Threat Hunting, da Sie nach Referenzen – in diesem Fall zu Pastebin – suchen können.

Mit der Storyline erstellt jeder autonome Endpoint-KI-Agent ein Modell seiner Endgerätestruktur sowie des Echtzeitverhaltens und weist ihm eine Storyline-ID zu, die einer Gruppe zusammenhängender Ereignisse zugeordnet wird. Durch die Suche nach „Pastebin" finden Sie eine Storyline-ID, die Sie schnell zu allen zugehörigen Prozessen, Dateien, Threads, Ereignissen sowie anderen Daten führt, die auf diese Anfrage zutreffen. Deep Visibility gibt vollständige, kontextualisierte Daten zurück, mit denen Sie schnell die Ursache der Bedrohung verstehen können, einschließlich ihres gesamten Kontexts, allen Beziehungen und Aktivitäten.

Jeder Endpoint-Agent kann einen Angriff automatisch oder manuell bereinigen, das System in seinen früheren Zustand zurückversetzen, es vom Netzwerk trennen oder eine Remote Shell im System nutzen. Das alles kann automatisch erfolgen – einfach mit einem Mausklick. Es dauert nur wenige Sekunden, erfordert keine Cloud-Verbindung und keine Datei-Uploads, die von Menschen ausgewertet werden müssen. Weil der Agent alles übernimmt, sind auch keine Cloud-Analysen nötig.

Die möglichst weitgehende Automatisierung löst mehrere Probleme: Erstens werden durch die Erkennung von schädlichem Verhalten dateibasierte Angriffe problemlos aufgedeckt, ohne dass dafür Signaturen erforderlich sind. Außerdem können so dateilose Angriffe verhindert und vorhergesagt werden.

Die Endpunkt-Sicherheit von SentinelOne greift bereits vor der Ausführung ein, um Angriffe noch vor der Durchführung aufzuhalten – ganz gleich, ob es sich um eine manipulierte PDF-Datei, ein Word-Dokument oder etwas anderes handelt. Der erste Schritt ist die Analyse, durch die ermittelt wird, ob die Datei irgendwie ungewöhnlich ist. Ist das der Fall, wird sie isoliert. Wenn der Code den ersten Test bestanden hat und die Ausführung beginnt, sucht ActiveEDR, der autonome, automatisierte Threat-Hunting-Mechanismus, der Funktionen für die Erkennung und Reaktion umfasst, nach ungewöhnlichen Verhaltensweisen. Er achtet beispielsweise auf Benutzer, die Word öffnen und damit eine PowerShell aufrufen und per Internetzugriff irgendetwas herunterladen. In den meisten Fällen ist das kein gutes, normales Verhalten. ActiveEDR sieht sich das Verhalten in Echtzeit an und erfasst alles, was innerhalb des Betriebssystems passiert, als einzelne Storyline – von Anfang bis Ende und unabhängig davon, ob sie nun eine Sekunde, einen Monat oder länger dauert. Die Technologie wägt ständig das Verhalten ab, um festzustellen, ob es eine negative Richtung einschlägt.

Menschliche Note durch verhaltensbasierte KI-Unterstützung

Das ist zwar gut, reicht aber nicht aus, weil es unmöglich ist, immer alles zu erwischen. Hier kommen die Threat-Hunting-Funktionen von ActiveEDR ins Spiel, durch die der Ansatz für dateibasierte und dateilose Angriffe von SentinelOne so überragend ist.

Angenommen, Sie haben ein Gerät gefunden, das mehrmals mit Pastebin kommuniziert hat. Wenn Sie auf die Storyline-ID klicken, gelangen Sie zur vollständigen Storyline des Angriffs mit allen relevanten Kontextinformationen. Sie sehen eine Übersicht zum Angriffsursprung und eine Prozessbaum-Zeitleiste mit den erzeugten Prozessen: Ein Microsoft Word-Dokument wurde geöffnet, eine Windows PowerShell wurde aufgerufen und diese Shell erzeugte dann selbst sieben weitere Prozesse. Die Storyline umfasst sogar komplette Befehlszeilenargumente, die zum vollständigen Verständnis benötigt werden. Enthalten sind auch vollständige Kontextinformationen zum Angriff, die nicht von einem kompletten Incident-Response-Team, sondern durch eine einzige Abfrage erstellt wurden.

Mit einem KI-Assistenten – zumal mit einem KI-Agenten auf jedem Gerät mit einer Netzwerkverbindung – sparen Sie erheblich Zeit. Dadurch ist Ihr Unternehmen nicht mehr ausschließlich darauf angewiesen, dass Mitarbeiter etwas analysieren müssen, das diesen Aufwand mitunter gar nicht Wert ist.

Sie können beruhigt schlafen: Wir schützen Sie!

Haben Sie sich nicht schon lange genug Sorgen gemacht? Das ist jetzt vorbei.

Sie können festlegen, dass die verhaltensbasierte KI Probleme automatisch behebt – und das macht enorm viel aus. Die Technologie ist in der Lage, direkt auf dem Gerät eine Entscheidung zu treffen – und zwar ohne Cloud-Verbindung und ohne dass ein Mensch ihr sagen muss, was zu tun ist. Wenn ActiveEDR sich im Erkennungsmodus befindet, erhalten Sie kontextualisierte Warnmeldungen. Im Schutzmodus wird ein entdecktes manipuliertes Word-Dokument einfach blockiert – menschliches Eingreifen ist nicht erforderlich. Wenn ein Benutzer versucht, die Word-Datei zu öffnen, wird die Bedrohung erkannt, blockiert und schnell entfernt. Wenn ActiveEDR sich im Schutzmodus befindet, zeigt die Storyline des Angriffs an, dass der Angriff nicht weit gekommen ist: Er wurde blockiert, bevor eine externe Kommunikation möglich war.

Weil diese verhaltensbasierten KI-Agenten in jedes Endgerät integriert sind, kann schädliches Verhalten gestoppt werden – und zwar sofort. Wenn Sie im Nachhinein entscheiden, dass etwas nicht blockiert werden soll, können Sie den früheren Zustand ganz leicht wiederherstellen. Im Gegensatz zum Menschen braucht ActiveEDR, die verhaltensbasierte KI von SentinelOne, keinen Schlaf und macht auch nicht um 17 Uhr Feierabend.

Die Realität der automatischen Bedrohungsbeseitigung mit verhaltensbasierter KI sieht so aus: keine Datenexfiltration, keine Schlagzeilen und kein Anruf von der Polizei.

Wenn Sie mehr über die verhaltensbasierte KI von SentinelOne und erfahren möchten, wie sie Ihr Unternehmen schützen kann, kontaktieren Sie uns oder fordern Sie eine kostenlose Demo an.

Like this article? Follow us on LinkedIn, Twitter, YouTube or Facebook to see the content we post.

Read more about Cyber Security

- MITRE-Manie: Was es mit der Anbieterpositionierung auf sich hat und worum es eigentlich geht