LEITFADEN

Die Handhabung modernen Endgeräteschutzes

Sechs Schritte zum besseren Schutz von Unternehmen heute und morgen

In dem Bestreben, Cyber-Kriminellen stets einen Schritt voraus zu sein, implementieren Unternehmen eine Schutzebene nach der anderen. Theoretisch sollten sie damit dann besser geschützt sein. Stattdessen aber ertrinken die Sicherheitsteams inzwischen regelrecht in Tools und Schnittstellen. Laut dem Forrester-Bericht ***Mastering the Endpoint*** (Die Herausforderung Endgerätesicherheit meistern) von 2017 sind in jedem Unternehmen inzwischen durchschnittlich zehn Agenten für Sicherheitslösungen aktiv, die es im Blick zu behalten gilt. Darüber hinaus jonglieren Firmen mit mindestens fünf verschiedenen Schnittstellen zur Untersuchung und Behebung von Zwischenfällen.

Um wirklich voranzukommen, muss Endgerätesicherheit neu durchdacht werden. Im Folgenden erläutern wir sechs grundlegende Schritte zur zeitgemäßen Handhabung von Endgeräten. Sie basieren auf realen Erfahrungen von über 250 Entscheidern in Sicherheitsfragen sowie Forschungsergebnissen von Forrester und McAfee. Mit diesen sechs Schritten sind Unternehmen heute und auch in Zukunft besser geschützt.

1. Bauen Sie eine Sicherheitsstruktur auf, die sich skalieren und an die sich stetig ändernde Bedrohungslage anpassen lässt.

Eine wachsende Zahl der Entscheidungsträger im Bereich der IT-Sicherheit bevorzugt integrierte Abwehrmechanismen in einem einzelnen, koordinierten System. Allerdings hat nur gut ein Drittel (35 Prozent) die Bedrohungsdaten auch so automatisiert, dass sie nutzbar sind.

Das Konzept der verschiedenen Sicherheitsebenen ist dabei weitgehend unumstritten. Der springende Punkt bei diesen Sicherheitsebenen ist jedoch, dass sie mittels eines flexiblen, adaptiven Sicherheits-Frameworks so miteinander verwoben werden müssen, dass sie den größten Nutzen bringen. Durch die Implementierung von Sicherheitsebenen, die untereinander Daten austauschen, erreichen Sie größere Leistung und einen höheren Wirkungsgrad.

Idealerweise lässt sich ein solches Framework erweitern, sodass Sie bei Bedarf neue Ebenen hinzufügen können, um auf Veränderungen in Ihrem Unternehmen sowie in Bezug auf Sicherheitsanforderungen zu reagieren.

2. Binden Sie Erkennungs- und Reaktionsmöglichkeiten in die tagtäglichen Geschäftsabläufe ein.

Dem Bericht zufolge kam es in den vergangenen zwölf Monaten in über der Hälfte der Unternehmen zu einem Cyber-Angriff, und die meisten betroffenen Unternehmen hatten danach vor allem damit zu kämpfen, die Kompromittierung sämtlicher infizierter Endgeräte zu beseitigen. Administratoren müssen die Möglichkeit haben, eine Bedrohung zu verfolgen und alle Geräte zu säubern, mit denen sie in Kontakt gekommen ist. In der Regel verfügen jedoch nur Spezialisten, von denen es schlicht nicht genügend gibt, über entsprechende Möglichkeiten.

Das Problem lässt sich auch mit einem weiteren modernen Programmpaket nicht beheben. Implementieren Sie deshalb eine Lösung, die Erkennungs- und Reaktionsmöglichkeiten in die täglichen Geschäftsabläufe einbindet. Damit haben Ihre Administratoren in der ersten Abwehrreihe die Möglichkeit zum schnellen Gegenschlag, wenn es zu Infektionen kommt – und diese sind unvermeidlich.

3. Minimieren Sie False-Positives, damit Sie sich auf die wirklich wichtigen Aufgaben konzentrieren können.

Laut der Forrester-Umfrage werden Genauigkeit und Vermeidung von False-Positives als das am dringendsten benötigte Leistungsmerkmal für Endgerätesicherheit eingestuft, dicht gefolgt von der Möglichkeit, Infektionen schon bei ihrem ersten Auftreten vollständig eindämmen zu können. Über 80 Prozent der Befragten sehen für sich allerdings auch erhebliche Hindernisse im Umgang mit Bedrohungen, etwa den Verwaltungsaufwand für Sicherheitslösungen und Schwierigkeiten bei der Priorisierung neu entdeckter Schwachstellen.

Die beste Antwort darauf ist eine verbesserte Koordination der Sicherheits-Tools mit dem Ziel, die Zahl der False-Positives zu verringern. Durch Bedrohungsschutz mit Datenaustausch lässt sich eine potenzielle Bedrohung automatisch als gefährlich oder ungefährlich einstufen, was die Administratoren entlastet. Durch die Verringerung der Komplexität und die Reduzierung manueller Schritte können die Sicherheitsteams in der ersten Abwehrreihe Wichtiges von Unwichtigem trennen und schneller reagieren. Bedrohungen lassen sich noch konzentrierter beheben, wenn Vorfälle mit höchster Priorität automatisch gemeldet und klare Abläufe zu deren Lösung angeboten werden.

4. Tauschen Sie Bedrohungsdaten in Echtzeit aus, und setzen Sie neue Erkenntnisse unverzüglich um.

Minutenaktuelle Bedrohungsdaten sind für den Schutz vor verschleierter Malware unerlässlich. Für die Aufdeckung von Gefahren, die den ersten Schutzmaßnahmen entgangen sind, setzen der Forrester-Umfrage zufolge 48 Prozent der Unternehmen auf Bedrohungsdaten. Fast ebenso viele Unternehmen verwenden Bedrohungsdaten-

Feeds, um Bedrohungen in ihrer IT-Umgebung aufzuspüren, Klarheit zu erlangen und Zusammenhänge zu erkennen.

Die ideale Strategie für eine Bedrohungsanalyse ist dabei eine Kombination aus externen Quellen und gesammelten Daten aus der eigenen IT-Umgebung. Auf Ihrer Plattform sollten die Bedrohungsdaten in Echtzeit zwischen den Sicherheitsebenen ausgetauscht werden – und das automatisch, ohne dass Administratoren erst mit Schnittstellen jonglieren müssen. Die aus einer Infektion gezogenen Schlüsse sollten dann von der jeweiligen Plattform aus an alle anderen Sicherheitssysteme in Ihrer IT-Umgebung weitergegeben werden.

5. Nutzen Sie hochentwickelte Machine Learning-Techniken und die Cloud, um die Schutzmaßnahmen zu skalieren und zu beschleunigen.

Laut der Forrester-Umfrage wird bei der Verwaltung der Endgerätesicherheit die Zeit zum Beziehen neuer Signaturen und manueller Updates für Endgeräte als größte Herausforderung empfunden.

Moderne Strategien verfolgen daher einen intelligenteren Ansatz: Mithilfe hochentwickelter, lokal sowie über die Cloud verfügbarer Machine Learning-Techniken können Sie verdächtige ausführbare Dateien mit tausenden Eigenschaften bekannter Bedrohungen statistisch vergleichen – ganz ohne Signaturen. Dank der Fähigkeit, statische Code-Merkmale ebenso zu analysieren wie das tatsächliche Verhalten einer ausführbaren Datei, lassen sich versteckte Bedrohungen binnen Sekunden aufdecken.

6. Konsolidieren Sie Software-Agenten und manuelle Prozesse.

Das Leben von Endgerätesicherheits-Administratoren ist nicht nur gefühlt komplizierter geworden: 81 Prozent der Befragten sehen für sich Hindernisse, die den effektiven Umgang mit Risiken erschweren.

Durch das Zusammenführen verschiedener Tools, Systeme und Berichte in einer einzigen Verwaltungskonsole lassen sich manuelle Prozesse drastisch verringern. Mit einem solchen Ansatz können Sie die Zahl der von Ihrem Team zu koordinierenden Agenten verringern und bislang manuelle Aufgaben durch optimierte Workflows automatisieren. Statt Ihr Team also stundenlang mit grundverschiedenen Schnittstellen kämpfen zu lassen, geben Sie ihm die Möglichkeit an die Hand, mehrere Endgerätesicherheitsebenen über automatische Einstellungen zu steuern, die nur einmal vorgenommen werden müssen.

Weitere Informationen

Wenn Sie mehr darüber erfahren möchten, wie Unternehmen auf Sicherheitslücken bei Endgeräten reagieren und welche Abhilfemaßnahmen Forrester empfiehlt, können Sie den **Bericht hier herunterladen**.

McAfee
Together is power.

Ohmstr. 1
85716 Unterschleißheim
Deutschland
+49 (0)89 3707 0
www.mcafee.com/de