STORMSHIELD

MEINUNGEN

ENDPUNKTSCHUTZ-LÖSUNG UND ANTI-VIRUS-SOFTWARE: WAS IST DER UNTERSCHIED?

Julien Paffumi
Product Portfolio Manager,
Stormshield

Fast ein Jahrzehnt nach dem angekündigten Ende traditioneller Anti-Viren-Programme stehen diese bei der breiten Öffentlichkeit nach wie vor hoch im Kurs. Als Begriff wird Anti-Viren-Software zwar häufig in der Computerwelt verwendet, es hat jedoch seinen guten Ruf verloren. Erfahren Sie, warum.

Der Einsatz herkömmlicher Anti-Viren-Programme scheint heute nicht mehr zeitgemäß zu sein, da die Begriffe „*Next-Generation Antivirus* (NGAV)", „EPP (*Endpoint Protection Platform*)" und „EDR (*Endpoint Detection and Response*)" immer mehr an Bedeutung gewinnen. Was sind die Unterschiede zwischen all diesen Erkennungstechnologien? Sind Anti-Viren-Programme heute noch erforderlich? Die Antworten auf diese Fragen finden Sie in diesem Artikel.

BIETEN ANTI-VIREN-PROGRAMME NOCH EINEN ZUVERLÄSSIGEN SCHUTZ?

Eine Anti-Viren-Software ist ein Computerprogramm zur Erkennung und Entfernung von Malware, das auf einzelnen Endgeräten wie Computern, Tablets oder Smartphones installiert werden kann. Der Begriff Anti-Virus wurde erstmals im Jahr 1987 von der Firma IBM als Antwort auf den Computervirus „Brain" entwickelt. **Er wurde im Laufe der Jahre durch viel Werbung populär und bildete in der Vorstellung der breiten Öffentlichkeit den einzigen Schutz vor Computerviren.**

Das Prinzip von Anti-Viren-Software beruht auf der Suche nach Signaturen. *„Ähnlich wie ein Impfstoff verfügt ein Anti-Viren-Programm über eine Signaturdatenbank, anhand derer es Computerviren erkennen kann. Deshalb war es unerlässlich, dass die Signatur des jeweiligen Virus zuvor generiert wurde*", erinnert sich **Stéphane Prévost**, Product Marketing Manager bei Stormshield. Diese Funktionsweise ist mit verschiedenen Problemen und Einschränkungen verbunden. Zunächst muss das Virus bekannt sein, bevor man seine Signatur identifizieren (und ihn bekämpfen) kann. Die zweite und wichtigste Einschränkung ist das Aufkommen des Polymorphismus, einer Technologie zur Erzeugung bösartiger Dateien, die jeweils über eine einzigartige digitale Signatur verfügen, deren Infektionsmethode und Auswirkungen jedoch gleich sind. Diese Einschränkung wird umso prägnanter, da täglich laut dem Institut AV-TEST 450.000 neue Malware-Programme entwickelt werden – das sind fast 4 Millionen pro Monat. Schlimmer noch für Anti-Viren-Software ist, dass sich die Vorgehensweisen der Cyberkriminellen in den letzten Jahren kontinuierlich weiterentwickelt haben. Sie nutzen blinde Flecken in den Erkennungsalgorithmen aus, wie z. B. bei Angriffen ohne Dateien (*fileless malwares*). Das Ergebnis? Der Erkennungsmechanismus, der auf der Suche nach digitalen Fingerabdrücken in einer Datei beruht, lässt eine große Mehrheit der Malware durch und muss unbedingt durch andere Sicherheitstechnologien ergänzt werden.

Die Entwicklung und Raffinesse von Cyberangriffen reicht sogar so weit, dass Anti-Viren-Programme selbst zur Zielscheibe werden. Auf der „Black Hat Europe"-Konferenz im Dezember 2022 enthüllte ein Sicherheitsforscher beispielsweise eine neuartige Schwachstelle, die mehrere Anti-Viren-Programme betrifft. Diese Sicherheitslücke ermöglicht es, Anti-Viren-Software zu kapern und sie dazu zu bringen, legitime Dateien zu löschen. Was kann man also tun, wenn das wichtigste Schutzinstrument seine Funktion nicht mehr erfüllt?

DER EINZUG DER VERHALTENSERKENNUNG IN SICHERHEITSLÖSUNGEN FÜR WORKSTATIONS

Um auf diese neue Bedrohung zu reagieren, mussten **die Hersteller von Cybersicherheitslösungen umdenken und von der Suche nach Fingerabdrücken zur heuristischen Analyse auf der Grundlage des Benutzerverhaltens wechseln**. Unter dem

Namen *Next-Gen Antivirus* oder NGAV bildeten diese neuartigen Anti-Viren-Programme die Grundlage für das spätere Konzept der EPP (*Endpoint Protection Platform*). EPP-Lösungen (*Endpoint Protection Platform*) waren eine erste Antwort auf Polymorphismus und dateifreie Angriffe, indem sie neue Funktionen wie Speicherüberwachung, Verhaltensanalyse oder die Überprüfung von Kompromittierungsindikatoren (IoCs) integrieren. Trotz dieses technologischen Fortschritts schlüpften heimtückische Cyberangriffe weiterhin durch die Maschen des Sicherheitsnetzes. Man erkannte, dass es unerlässlich ist, Angriffe auch im Nachhinein noch zu erkennen und darauf zu reagieren.

So tauchten im Jahr 2013 *Endpoint Threat Detection & Response*-Lösungen (ETDR) in den Analysen von Gartner rund um die Themen Incident Response und Investigation auf. Ab 2015 wurde das Akronym ETDR durch EDR für *Endpoint Detection & Response* ersetzt. Die Besonderheit dieses neuen Ansatzes liegt in der Fähigkeit, unbekannte Bedrohungen zu erkennen und in Echtzeit halbautonom darauf zu reagieren, wie **Noël Chazotte,** Product Manager Stormshield, betont: „*Wenn eine Bedrohung erkannt wird, blockiert die Anti-Viren-Software das Programm im Vorfeld – manchmal wird es auch unter Quarantäne gestellt. EDR tritt in Aktion, wenn der Sicherheitsvorfall entdeckt wird oder bereits auf dem Rechner aufgetreten ist, und versucht festzustellen, was genau geschehen ist. So unterstützt es Einsatzteams dabei, eine weitere Ausbreitung der Infektion zu verhindern.*"

Wie erkennt die EDR-Technologie ausgefeilte Angriffe? „*EDR erkennt ungewöhnliche Verhaltensweisen anhand von Kompromittierungsindizes (IoC)*", erklärt Stéphane Prévost. *Dabei muss es sich nicht immer um außergewöhnliche Ereignisse handeln, sondern es können auch banale Aktionen sein, wie das Herstellen einer Verbindung zu einem externen Server*. „Deshalb ist es wichtig, den Funktionsrahmen der Lösung während der Lernphase genau zu definieren, um Fehlalarme (sog. False Positives) zu vermeiden. Aber EDR- und EPP-Lösungen bleiben weiterhin komplementär, wie Stéphane Prévost betont: „*Man kann eine Parallele zur physischen Sicherheit eines Unternehmens ziehen. EDR-Lösungen stellen Überwachungskameras dar: Mit ihnen können Sie sehen, ob z. B. eine Person in Ihr Firmengelände eindringt. Aber um den Eindringling schon am Eingang abzuwehren, benötigen Sie einen Wachmann vor Ort: das ist EPP.*"

Und welche Rolle spielt Anti-Viren-Software bei alledem? Laut security.org glauben drei von vier Amerikanern, dass sie im Jahr 2023 ein Anti-Viren-Programm benötigen, um ihren privaten Computer unbesorgt nutzen zu können. Angesichts der oben erwähnten technologischen Fortschritte stellt sich auf professioneller Ebene jedoch die Frage: **Warum brauchen wir heute überhaupt noch Anti-Viren-Programme?** Und die Antwort lautet: Ja, denn sie bieten eine erste Sicherheitsebene. Auch wenn diese Software nicht gegen alle Cyberangriffe wirksam ist, bietet sie dennoch einen ersten Schutz vor weniger raffinierten Angriffen – mit der Garantie, dass die Problematik von False Positives vermieden wird, und mit einem sehr geringen Ressourcenverbrauch auf dem Computer. Doch eine erste Sicherheitsebene reicht nicht aus. „Es lässt sich beobachten, dass auf ein und demselben Computer mehrere Sicherheitslösungen installiert werden", erklärt Noël Chazotte. „*Diese Kombination verträgt sich jedoch nicht immer gut, und einige Konstellationen können zu Konflikten führen, wodurch Cyberkriminellen eine weitere Tür geöffnet wird.*"

NDR, XDR, MDR: AUF DEM WEG ZUR SPEZIALISIERUNG DER ERKENNUNG & REAKTION

Trotz der versprochenen Autonomie solcher Lösungen müssen diese Tools von Experten betreut werden, wie die Entwicklung von Angeboten für Managed EDR oder Mini-SOCs zeigt. **Neben der Verbesserung der Erkennung müssen Tools zum Endpunktschutz unbedingt auch über die Fähigkeit verfügen, Vorfälle zu erkennen und darauf zu reagieren.** Und da es immer mehr Sammelstellen für Vorfälle gibt, müssen SOC-Analysten Zugriff auf alle Netzwerk- und Infrastrukturgeräte haben.

So analysieren NDR-Lösungen (*Network Detection and Response*) die TCP/IP-Pakete, die über das Netzwerk versendet werden, um verdächtige Aktivitäten zu erkennen, während XDR-Plattformen (*eXtended Detection and Response*) dazu dienen sollen, alle internen und externen IT-Assets (Netzwerk, Verzeichnisse, Cloud-Ressourcen, Firewalls usw.) zusammenzuführen. Dies bietet einen Gesamtüberblick über die Ereignisse innerhalb des IT-Systems. Für Noël Chazotte ist *„eine XDR-Plattform eine Kollektion von Sammelpunkten und vor allem eine Korrelationsplattform, die dazu beiträgt, das Risiko zu mindern und auf Vorfälle zu reagieren und sie zu beheben."*

In den letzten Jahren sind andere Akronyme, wie beispielsweise MDR, entstanden. In der Praxis entspricht *Managed Detection and Response* (MDR) lediglich einer Vermarktungsform von XDR, bei der ein externes Team die Warnmeldungen bearbeitet. Unabhängig von Tools und Technologien sollte man sich stets vor Augen halten, dass Analysten weiterhin eine zentrale Rolle spielen und dass keine Technologie allein sensible Vermögenswerte schützen kann.

In einer Studie der Organisation Survey Risk Alliance gaben nur 12 % der Fachleute für Cybersicherheit an, dass sie bis 2022 eine XDR-Lösung in ihrer Organisation eingeführt hatten. Die restlichen 77 % sagten, dass sie die Einführung in den nächsten 24 Monaten planten. Die Nachfrage nach Sicherheitsfachleuten, die sich auf die Erkennung und Reaktion auf Vorfälle spezialisiert haben, dürfte folglich in den nächsten Jahren weiter steigen. Diese Fähigkeiten werden dringend benötigt, um mit der ständigen Weiterentwicklung der Vorgehensweisen Schritt zu halten, und ihre Dienste werden für Unternehmen wahrscheinlich leichter zugänglich sein, wenn sie Managed EDR oder Mini-SOCs nutzen.