N-ABLE™

EDR und Antivirus:
Gemeinsamkeiten und Unterschiede

E-Book

Einleitung

Sicherheit auf mehreren Ebenen ist die beste Verteidigung angesichts der Gefahren, denen die Netzwerke Ihrer Kunden auch künftig ausgesetzt sein werden. Im Rahmen dieses Modells ist häufig die Rede von zwei Sicherheitslösungen für Endpunkte – Antivirus (AV) und Endpoint Detection and Response (EDR). Jede Technik hat ihre Vorteile, doch worin genau unterscheiden sich beide? Und wird Virenschutz, wie wir ihn kennen, schon bald Geschichte sein? Wir erklären Ihnen die Sachlage.

Entweder – oder

AV und EDR konkurrieren im System um Ressourcen. Ihre gleichzeitige Verwendung auf einem Endgerät kann zu Problemen führen, weshalb wir davon abraten. Am besten installieren Sie also pro Endgerät entweder das eine oder das andere.

Bei Ihrer Entscheidung sollten Sie mehrere Faktoren berücksichtigen, darunter die Art des Unternehmens, das geschützt werden muss, die Endbenutzer und die Kosten. Einige Kunden müssen vielleicht dieselbe Lösung für ihren gesamten Benutzerstamm verwenden. Andere wiederum setzen lieber auf eine gezielte Absicherung bestimmter Geräte mit EDR und schützen den Rest über AV. Wie dem auch sei: N-able bietet beide Lösungen an.

AV: Solider Schutz zum günstigen Preis

AV schützt Kundensysteme vor Malware. AV-Programme nehmen automatisch regelmäßige Updates von Software und Virendefinitionen vor. Darum kümmern Sie sich als Serviceanbieter, Ihre Kunden müssen nichts unternehmen. Erkennt der Virenschutz Malware oder einen Virus, wird dieser umgehend in Quarantäne verschoben. Viele Jahre lang war AV der Standardschutz vor Malware. Fast alle wissen, was ein Virenscanner ist, deshalb ist diese Technik auch einfacher zu verkaufen.

Der Nachteil: AV-Programme benötigen regelmäßige Updates der Virensignaturen. Von der Qualität dieser Updates hängt es ab, wie gut diese Programme schützen. Täglich treten neue Gefahren auf und idealerweise stehen die Signatur-Updates immer rechtzeitig auf den Endgeräten zur Verfügung. Tatsächlich werden Bedrohungen aber oft erst erkannt, wenn sie bereits Schaden angerichtet haben. Hinzu kommt, dass AV-Software nur gegen Viren und Schadsoftware schützt – bei Weitem nicht die einzigen Bedrohungen für einen Endpunkt. Immer häufiger gibt es beispielsweise dateilose Angriffe. Diese werden jedoch von einem AV nicht erkannt.

Außerdem nutzen Kriminelle zunehmend Methoden, mit denen der AV-Schutz umgangen werden kann. Wie etwa Packer, die die Malwaredateien verschlüsseln und dadurch schwer erkennbar machen. Oder sie setzen Malware mit immer wieder frischen Signaturen ein, die in noch keiner Datenbank erfasst sind und deshalb vom Virenscanner nicht erkannt werden. Kriminelle Hacker arbeiten bereits seit Jahren an der Umgehung des nur zu gut bekannten AV-Schutzes. Dabei ist ein AV beileibe nicht wehrlos (viele Lösungen erkennen wirklich einen Großteil der bekannten Viren), doch er hat eben Schwachstellen.

Wenn dem so ist, was spricht dann überhaupt für Managed AV? Zuerst einmal: Ein AV bietet Endbenutzern immer noch soliden Schutz vor Bedrohungen aus dem Internet. Und wenn Sie den AV-Schutz für sie verwalten, müssen sich die Benutzer nicht mehr selbst darum kümmern. Womöglich am stärksten punktet der AV-Schutz allerdings mit seinem Kostenvorteil. Pro Gerät kommt AV günstiger als EDR – für preissensible Kunden ein Argument. Allerdings gilt: Ihre eigene Gewinnspanne ist bei AV oft eher mäßig. Außerdem rechtfertigt sich die Investition in EDR von ganz alleine, wenn man bedenkt, welche Kosten ein Cyberangriff nach sich ziehen kann.

EDR: Eine neue Dimension der Endgeräteabsicherung

EDR bietet mehrere Facetten. Es kann alles, was auch AV leistet, und noch einiges mehr. Die Lösung verbessert also nicht nur die Sicherheit, sondern schont auch die Nerven Ihrer Kunden. Wie bei AV liegt auch bei EDR alles in Ihrer Hand als MSP – Ihre Endbenutzer müssen nichts tun. Sobald eine große Zahl an Endgeräten geschützt werden soll, erweisen sich klassische AV und andere Punktlösungen angesichts der täglich zunehmenden Bedrohungen als eher umständlich.

Auch EDR zielt auf den Schutz von Endpunkten ab, doch die Technik erkennt nicht nur Malware. Auf der Basis von Monitoringsoftware und Endpunkt-Agenten setzt eine EDR-Lösung auch maschinelles Lernen und künstliche Intelligenz (KI) ein: Damit behält sie nicht nur Dateien im Blick, sondern kann auch verdächtiges Verhalten erkennen und rechtzeitig eingreifen, bevor es zu Schäden kommt.

AV kann Malwaredateien hervorragend abwehren. Gegen dateilose Angriffe kann die AV-Software hingegen nichts ausrichten. So könnten Hacker etwa offene RDP-Ports dazu verwenden, um ein neues Administratorkonto anzulegen, sich auf dem betreffenden Endpunkt festzusetzen und Änderungen daran vorzunehmen, von denen der MSP oder der rechtmäßige Administrator erst einmal nichts mitbekommt. Gegen solche Angriffe sind herkömmliche Virenschutzprogramme machtlos. EDR kann auch verdächtige Aktivitäten erkennen und melden. Wenn beispielsweise mehrere Dateien auf einem Endpunkt gleichzeitig geändert werden und dies untypisch ist, können EDR-Lösungen das Verhalten melden, den Administrator warnen und ihm die Möglichkeit geben, Maßnahmen zu ergreifen. Auch brandneue Bedrohungen, die in der Sicherheitscommunity noch nicht die Runde gemacht haben, können dank EDR entlarvt werden. Normale AV-Lösungen, die mit Signaturen arbeiten, haben hier eine Schwachstelle. Der signaturlose EDR-Ansatz bietet Abhilfe.

Bei EDR-Lösungen erfolgt die Behandlung direkt auf dem Endpunkt, anstatt die Gefahrenanalyse und -behandlung ressourcen- und zeitaufwändig über die Cloud laufen zu lassen. Auf diese Weise erkennen Sie Bedrohungen umgehend und können schneller reagieren.

Zu konstatieren, dass eine Bedrohung Schaden angerichtet hat, reicht nicht – Sie sollten außerdem wissen, auf welche Weise es geschehen ist und wie es zur Kompromittierung des Endpunkts kommen konnte. Hier liegt der wahre Vorzug von EDR – die aktive Ursachenanalyse. EDR-Lösungen können den Verlauf eines Angriffs illustrieren; Sie sehen quasi seine visuelle Storyline. Sie erkennen, über welchen Prozess der Angriff landen konnte, wie sich die Malware vermehrt und verbreitet hat und wie sie aufgebaut ist, und erhalten so aussagekräftige Daten, auf deren Grundlage Sie die Sicherheit der von Ihnen betreuten Systeme weiter verbessern können.

Sie können in Echtzeit mitverfolgen, wie sich der Verlauf des Angriffs entwickelt, doch mit EDR sind Sie dem Vorgang nicht hilflos ausgeliefert. EDR bietet Ihnen im Fall eines Angriffs mehrere Handlungsoptionen – je nach der pro Endbenutzer getroffenen Einstellung: Löschen, Quarantäne, Behebung und Rollback. Stellen Sie sich N-able EDR als Ihr persönliches Sicherheitscenter vor, von dem aus Sie Schäden buchstäblich ungeschehen machen und Ransomware ihren Schrecken nehmen können.

Obwohl AV anfangs vielleicht pro Lizenz etwas weniger kostet, könnte der potenzielle Nachteil eines weniger robusten Schutzes enorm sein. So sind Ransomware-Angriffe zum Beispiel weit mehr als nur ein Ärgernis. Sie müssen die Produktivitätszeit, die Kosten für die Wiederherstellung von Endpunkten, den Imageschaden durch Ausfallzeiten und sogar mögliche Geldstrafen aufgrund von Datenschutzgesetzen berücksichtigen. Die Vermeidung all dieser Kosten kann die Mehrinvestition für EDR bei Weitem aufwiegen. Da Internetbedrohungen immer gefährlicher und kostspieliger werden, könnte sich EDR langfristig durchaus als Standard etablieren.

Zusammenfassung

EDR-Lösungen bieten zahlreiche der Vorteile einer AV-Lösung, aber darüber hinaus noch vieles mehr:

- **Proaktive Erkennung:** AV-Lösungen sind auf eine aktuelle Signaturdatenbank angewiesen und nehmen Scans nach Zeitplan vor. EDR hingegen nutzt KI und maschinelles Lernen zur Erkennung potenzieller Gefahren und schließt so gefährliche Sicherheitslücken.
- **Erkennung einer größeren Bandbreite an Bedrohungen:** EDR erkennt nicht nur Viren und Malware, sondern auch verdächtigen Datenverkehr und dateilose Angriffe.
- **Ursachenanalyse:** EDR illustriert die zeitliche Entwicklung verdächtiger Verhaltensweisen. So erhalten Sie genaueren Einblick in das Angriffsgeschehen und können Ihre Sicherheitssteuerung so anpassen, dass das Problem nicht erneut auftritt.
- **Schnelle Abhilfe:** Mit EDR können Sie Bedrohungen schnell beseitigen. So können Sie beispielsweise nach einem Ransomware-Angriff einen Endpunkt direkt von der EDR-Lösung aus in einen sicheren Zustand zurückversetzen.

Über N-able

N-able bietet MSPs und IT-Serviceanbietern leistungsstarke Software zur Überwachung, Verwaltung und Absicherung von IT-Infrastrukturen und Netzwerken. Unser Angebot umfasst eine skalierbare Plattform, eine sichere Infrastruktur, Tools für die einfachere Verwaltung komplexer IT-Umgebungen und Ressourcen für die digitale Transformation. Wir unterstützen unsere Partner in jeder Wachstumsphase beim Schutz ihrer Kunden sowie beim Ausbau ihres Angebots – durch das ständig wachsende flexible Portfolio an Integrationen führender Anbieter.

n-able.com/de