N-ABLE™

Endpoint Detection and Response – Virenschutz in neuer Dimension

E-Book

Ransomware. Zero-Day-Malware. Dateilose Angriffe. Phishing, gekaperte Admin-Konten.

All dies bedroht die IT-Systeme und personenbezogenen Daten Ihrer Kunden und bringt ihren Geschäftsbetrieb in Gefahr.

Jahrelang konnten Sie zum Schutz der Endpunkte in den von Ihnen betreuten Netzwerken bedenkenlos Antivirus-Lösungen (AV) einsetzen. Doch angesichts zahlloser neuer Bedrohungen zeigen sich nun ihre Schwachstellen, für deren Behebung inzwischen neue Lösungen entwickelt wurden.

In den letzten Jahren ist immer häufiger von Endpoint Detection and Response, kurz EDR, die Rede – also von Endgeräteerkennung und Vorfallsbehandlung. EDR-Lösungen wurden speziell auf den Markt gebracht, um die Systeme an die sich ständig verändernde Bedrohungslandschaft anzupassen – in dem Bewusstsein, dass sich die Lage schneller weiterentwickeln wird, als der Mensch mithalten kann. Sind Sie neugierig, was es mit diesen Lösungen auf sich hat und inwiefern sie sich von anderen unterscheiden?

Im Folgenden werden wir Sie mit diesen Lösungen vertraut machen und Ihnen erklären, warum EDR für die Zukunft der Cybersicherheit unerlässlich ist.

Was genau ist EDR?

Anton Chauvin von Gartner® hat den Begriff „Endpoint Detection and Response“ (EDR) geprägt und damit eine Familie neuer Tools beschrieben, deren Schwerpunkt auf Sichtbarkeit und Prävention bis hin zur Erkennung von Endgeräten liegt.[1] EDR ist eine vielseitige Lösung, mit der AV in einen völlig neuen Bereich integriert wird. EDR kann alles, was auch AV leistet, und noch vieles mehr. Die Lösung verbessert also nicht nur die Sicherheit, sondern auch das Sicherheitsgefühl. Die wichtigsten Funktionen von EDR:

- Monitoring
- Gefahrenerkennung
- Die Möglichkeit, Listen zu erstellen und Auflistungen zu sperren/auszuschließen
- Gefahrenbehandlung
- Integration in andere Cybersicherheitslösungen

EDR-Lösungen greifen auf mehreren Ebenen, wodurch IT-Anbieter und IT-Experten ihren Benutzern einen umfassenderen Schutz bieten können – vom Einsatz künstlicher Intelligenz (KI) zur Überwachung und Erkennung neuer Bedrohungen oder verdächtiger Verhaltensweisen am Endpunkt bis hin zum automatischen Rollback nach einem Ransomware-Vorfall.

[1] „A Short History of EDR“, Reed Exhibitions Ltd. infosecurity-magazine.com/opinions/history-edr/ (aufgerufen im September 2020).

Die Rolle der EDR im Cybersecurity-Universum

EDR dient dem Schutz von Endpunkten. Ist deren Zahl sehr groß, sind klassische AV-Lösungen und andere traditionelle Sicherheitslösungen für Endpunkte angesichts der täglich zunehmenden Bedrohungen zuweilen überfordert. Traditionelle AV-Lösungen sind passiv. Sie können nur bereits bekannte Viren erkennen und in Quarantäne versetzen – Malware also, die zuvor schon einmal als solche entdeckt wurde.

Viele AV-Lösungen funktionieren auf Basis sogenannter Virensignaturen. Wenn eine Malware-Datei entdeckt wird, wird ein Hash erzeugt, der zu einer Virensignatur-Datenbank hinzugefügt wird. AV-Programme scannen Systeme nach Dateien ab, die zu bereits erfassten Virensignaturen passen. Finden sie eine solche Datei, dann wird diese unter Quarantäne gestellt.

Dass diese Signaturen regelmäßig aktualisiert werden müssen, ist ein Schwachpunkt dieser Technik. Zwischen dem Moment, in dem ein neues Virus zum ersten Mal entdeckt wird, und dem Zeitpunkt, zu dem Sie Ihre Kunden wirksam davor schützen, liegt ein mehr oder minder großes Zeitfenster. Bevor das nächste Signatur-Update kommt, kann bis dahin noch unbekannte Malware unerkannt in Systeme eindringen und dort Schaden anrichten. Anders gesagt: Der AV-Ansatz ist rein reaktiv.

EDR hingegen ist proaktiv. Hier gibt es eine Monitoringsoftware und Endpunkt-Agenten. Dank integriertem maschinellem Lernen und ausgefeilter künstlicher Intelligenz (KI) kann die Lösung verdächtiges Verhalten erkennen und handeln – auch ohne einen Signatureintrag dazu. Werden beispielsweise mehrere Dateien gleichzeitig geändert, erkennt die EDR darin eher einen Angriff auf einen Endpunkt als einen Benutzerfehler.

Aber auch das Treiben der Hacker ist proaktiv. Sie suchen nach Wegen, herkömmliche AV-Scanner auszutricksen. Beispielsweise durch regelmäßige Veränderung des Hash-Wertes einer Malware, so dass dieser beim Datenbankabgleich nicht gefunden wird. Weitere beliebte Maschen sind dateilose Angriffe oder die Einrichtung neuer Administratorkonten auf Endpunkten mit umfassenden Rechten. Eine EDR-Software hält nach Prozessen Ausschau, die auf Endpunkten vergleichsweise ungewöhnlich sind, und reagiert dann entsprechend. Hacker mögen proaktiv sein. Mit EDR sind Sie es aber auch.

AV kann nur bekannte Bedrohungen erkennen und unter Quarantäne stellen – also die, die zuvor identifiziert wurden.

Wandel – die einzige Konstante

Die Welt wandelt sich fortlaufend, so auch die Technik. E-Commerce-Services oder Unternehmensanwendungen werden tagtäglich von Milliarden Menschen genutzt: Die Cloud hat unser aller Leben gewaltig verändert. Doch Kriminelle halten mit der technischen Entwicklung Schritt und nutzen jede Neuerung, um an wertvolle Daten heranzukommen. Daten aber sind das höchste Gut Ihrer Kunden. Was unternehmen Sie, um sie zu schützen?

Nicht nur die Cloud hat die Wirtschaft und das Leben verändert, auch künstliche Intelligenz und maschinelles Lernen werden es tun. Hinter EDR-Lösungen stehen KI und maschinelles Lernen. Auf dieser Basis sorgen sie für besseren Schutz vor Bedrohungen und eine Erkennung und Behandlung auch ausgefeilter Bedrohungen.

Durch maschinelles Lernen analysiert die EDR zuerst die grundlegenden Verhaltensmuster eines bestimmten Endgeräts und erkennt auf dieser Grundlage dann Aktivitäten, die davon abweichen. Hierin liegt die besondere Stärke dieser Lösung. Sie analysiert Folgendes:

- Wurde die betreffende Aktion auf diesem Endpunkt schon einmal ausgeführt?
- Ist an einer Datei oder einem Verhalten etwas ungewöhnlich?
- Warum werden gesicherte Dateien angezeigt oder angegriffen?

Die KI hilft EDR-Lösungen also dabei, Indizien für einen Angriff auch ohne Rückgriff auf bereits bekannte Charakteristika zu erkennen – ein Prinzip, das ohnehin ganz einfach unterlaufen werden kann. Polymorphe Malware erstellt neue Versionen ihrer selbst, um nicht entlarvt zu werden, Zero-Day-Malware nutzt bislang unbekannte Sicherheitslücken. Diese Schädlinge können traditionellen AV-Lösungen durch die Lappen gehen. Die EDR wiederum leistet nicht nur die relevanten Analysen, sondern ergreift auch konkrete Maßnahmen gegen Malware-Angriffe: Prozessabbruch, Quarantäne, Behebung und Rollback.

Reaktionsmöglichkeiten von EDR-Lösungen

EDR-Software entdeckt Bedrohungen nicht nur, sie kann sie auch behandeln. Sobald ein Endpunkt-Agent eine Malware entdeckt, wird eine gute EDR sofort aktiv über das zentrale Monitoringsystem, das die Bedrohungen analysiert und korreliert. Bei einigen Lösungen können Sie die Entstehung des Angriffs und seinen Weg zum Endpunkt sogar visuell verfolgen. Ein Blick auf den zeitlichen Verlauf des Angriffs hilft Ihnen, seinen Lebenszyklus zu verstehen. Sie können diese Informationen nutzen, um zukünftige Bedrohungen zu unterbinden. Diese Darstellung ist auch äußerst nützlich, um den Kunden den Wert Ihrer Sicherheitsdienste zu demonstrieren.

AV und Festplattenverschlüsselung sind eine mögliche Methode für die Absicherung von Endpunkten. EDR hingegen bietet Ihnen Absicherung, die auch zukunftstauglich ist: Sie erhalten Analysen und Warnmeldungen in Echtzeit und detaillierte forensische Daten. Sie haben die Möglichkeit, Geräte offline zu schützen oder sie vom Netzwerk zu trennen, um die Weiterverbreitung eines Befalls zu unterbinden und – als allerwichtigste Funktion – den Rollback befallener Dateien.

Lassen Sie uns einen Blick darauf werfen, wie EDR bei Ransomware helfen kann. Ein Ransomware-Angriff läuft meist wie folgt ab: Ein Benutzer öffnet eine E-Mail, einen E-Mail-Anhang oder besucht eine betrügerische Website. Plötzlich wird auf seinem Bildschirm eine Meldung angezeigt, dass alle Dateien auf dem Computer verschlüsselt werden und der Betreffende sie nur zurückbekommt, wenn er in Bitcoin oder einer anderen Kryptowährung ein Lösegeld zahlt. Ohne Garantie, dass er danach seine Daten zurückbekommt, versteht sich. Deshalb sind viele Unternehmen nicht bereit, das Risiko einer Zahlung einzugehen.

EDR mit Ransomware-Rollback-Funktionen bietet Ihren Kunden enormen Mehrwert. Mit Hilfe einer ganz besonderen Technik nimmt die Funktion in regelmäßigen, vom Admin konfigurierbaren Intervallen Snapshots des betreffenden Endpunkts auf. Schlägt eine Ransomware zu, so kann das Geräte-Image mit wenigen Klicks auf einen vorherigen Zeitpunkt zurückgesetzt werden – eine enorme Zeit- und Geldersparnis für Ihre Kunden.

Ist EDR für Sie und Ihre Kunden das Richtige?

Nehmen Sie Ihre eigenen Möglichkeiten und die Bedürfnisse Ihrer Kunden genauer unter die Lupe, bevor Sie sich für oder gegen EDR entscheiden. Wie bereits erwähnt, ist EDR nicht der einzige sinnvolle Weg, Endpunkte abzusichern. Entscheidend ist, mit welchen Daten und Anwendungsbeispielen Sie es zu tun haben. Müssen sensible Daten geschützt werden, etwa auf dem Computer eines Personalmitarbeiters (der mit Sicherheit auch personenbezogene Daten verwaltet), dürfte EDR ideal sein. Für Geräte mit einer Cloudspeicherung persönlicher Benutzerdaten und mit Schutz durch Backup, Festplattenverschlüsselung und AV ist sie womöglich nicht nötig.

Sprechen Sie auch bei preisbewussten Kunden einen möglichen Schutz durch EDR an – es kann sich durchaus lohnen. Vielleicht ziehen Sie sogar in Erwägung, die Verwendung von EDR für Ihre Kunden dringend zu empfehlen (oder sogar zur Bedingung zu machen). Denn die Rollback-Funktion ist beispielsweise im Fall von Ransomware-Angriffen wirklich Gold wert: EDR erkennt und stoppt den Ransomware-Angriff sofort. Betroffene Endpunkte werden binnen Sekunden wiederhergestellt und die Ransomware daran gehindert, sich im Netzwerk weiterzuverbreiten. So lassen sich größere Systemausfälle verhindern und Ihre Kunden können viel Zeit und Kosten sparen. Und insgesamt ist der Schutz durch EDR einfach umfassender als durch AV. EDR mag nicht die einzige Sicherheitsoption sein, aber es lohnt sich, das Gespräch mit Ihren Kunden zu führen, um sie möglicherweise aktiv in Richtung eines umfassenderen Schutzes zu führen.