N-ABLE™

EDR oder Antivirus:
Welche Lösung ist die richtige für Sie?

E-Book

EDR oder Antivirus:
Welche Lösung ist die richtige für Sie?

Sowohl Antivirus-(AV)-Lösungen als auch Endpoint-Detection-and-Response-(EDR)-Lösungen schützen Endpunkte vor Cyberbedrohungen – allerdings auf unterschiedliche Weise. Hier finden Sie eine kurze Zusammenfassung der wichtigsten Unterschiede.

AV – Antivirensoftware:

- Schutz gegen Malware und Viren. In der Regel durch das Scannen von Dateien.
- Traditionell basiert dies auf Virensignaturen. Das bedeutet, dass der AV-Anbieter die bösartige Software zuerst entdeckt und ein Signatur-Update an die Benutzer übermittelt haben muss, und natürlich auch, dass die Endbenutzer ihre Virensignaturen auf dem neuesten Stand halten müssen.
- Der Administrator muss regelmäßig Virenscans vornehmen.
- Preislich allgemein günstiger als EDR.

EDR – Endgeräteerkennung und Vorfallsbehandlung:

- Schutz gegen verschiedene Bedrohungen: dateilose Angriffe, infizierte Dokumente und schädliche Skripte. Beobachtet Geräteverhalten unter Einsatz von künstlicher Intelligenz.
- Hält nach möglichen Angriffsversuchen Ausschau, statt sich auf Dateiscans zu verlassen. Wenn EDR verdächtige Vorgänge auf einem Endgerät erkennt, wird (erforderlichenfalls) eine Warnmeldung ausgegeben.
- Behandelt potenzielle Bedrohungen automatisch. Manche EDR-Lösungen können Windows-Endpunkte nach einem Ransomware-Angriff in kürzester Zeit wieder in einen sicheren, einwandfreien Zustand zurückversetzen.
- Kostet etwas mehr als klassische AV-Software.

EDR bietet umfassenderen Schutz gegen Internetgefahren sowie mehr Möglichkeiten für eine angemessene Reaktion darauf. Man sollte meinen, dass deshalb alles für EDR und kaum etwas für AV spricht. Tatsächlich gibt es jedoch sowohl für EDR als auch AV sinnvolle Einsatzszenarien. Doch wie entscheiden Sie, welche Lösung jeweils richtig ist?

Die Risiken abwägen

Der umfassende Schutz, den EDR-Lösungen bieten, sichert die Systeme Ihrer Kunden unterm Strich lückenloser ab. Daher sollten Sie Ihren Kunden bevorzugt EDR anbieten, denn deren Endpunkte werden damit schlicht besser geschützt. Ihnen wiederum bringt EDR ein Umsatzplus, denn Ihre Kunden müssen dafür ja tiefer in die Tasche greifen als für AV.

Doch nicht jeder Kunde möchte mehr bezahlen – da ist eine pragmatische Herangehensweise gefragt. Am besten ermitteln Sie also, welches Risiko der betreffende Kunde hat, und

überlegen dann gemeinsam ein sinnvolles Vorgehen. Bei risikobasierten Ansätzen geht es in der Regel darum, Ressourcen für Sicherheit und technische Administration zu bewahren oder Lücken in Endbenutzersystemen zu schließen (etwa durch Multifaktor-Authentifizierung für systemrelevante Personen wie Führungskräfte oder Systemadministratoren). Doch der Blick aufs Risiko kann auch finanzielle Entscheidungen erleichtern.

Letztlich müssen Sie überlegen, welche Endbenutzer geschützt werden sollen, ob sie Zugriff auf sensible Daten haben und welche Folgen der Verlust dieser Daten hätte.

Die folgenden Nutzertypen mögen Ihnen als Orientierungshilfe dienen:

- **Personalmanager:** Auf dem Computer dieses Benutzertyps befinden sich mit hoher Wahrscheinlichkeit personenbezogene und damit vertrauliche Daten. Er hat Zugriff auf Gehaltsabrechnungen, Sozialversicherungsnummern, Mitarbeiteradressen und potenziell sensible Informationen über Arbeitsverträge usw. Geraten diese Daten in die Hände Krimineller, kann der Schaden für das Unternehmen und die betroffenen Personen groß sein. Endgeräte, auf denen sich solche Daten befinden, wären durch AV nicht ausreichend geschützt. Hier wäre es gut, wenn eingeschleuste Malware nicht nur in Quarantäne verschoben, sondern sofort gelöscht wird und das befallene Gerät vom Netzwerk getrennt werden könnte, um die Weiterverbreitung des Schädlings zu unterbinden. Für diesen Benutzertyp kommt nur EDR in Frage; die höheren Kosten dafür sind durch die hier bestehenden Risiken und potenziellen Folgekosten eines erfolgreichen Angriffs vollauf gerechtfertigt.
- **Grafiker:** Auf dem Computer dieses Benutzertyps befinden sich durchaus wichtige Geschäftsdaten, wahrscheinlich aber keine nennenswerte Menge an personenbezogenen Daten. Kurzum, eine Kombination aus Antivirus, Backup und Festplattenverschlüsselung dürfte hier völlig ausreichend sein. Zwar würde EDR natürlich umfassender schützen, doch das hier bestehende Risiko ist durch eine preislich günstigere Antivirus-Lösung bestens abgedeckt.
- **Unternehmensleitung, Topmanager:** Dieser Benutzertyp fällt in puncto Datenschutzverletzung in der Regel in die höchste Risikokategorie, weil sich auf seinem Computer höchstwahrscheinlich personenbezogene Daten und äußerst wertvolle Geschäftsdaten befinden. Die Daten auf solchen Computern bedürfen eines lückenlosen Schutzes, sollten aber im Fall der Fälle auch zügig per Rollback rückholbar sein. Es besteht auch die Möglichkeit, dass jemand eine Fernverbindung zum Computer des Geschäftsführers herstellt und entweder schwer zu entdeckende Spyware installiert oder ohne das Wissen des Benutzers ein Superadmin-Konto einrichtet. So könnte sich ein Cyberkrimineller mühelos Zugang zu weiteren Teilen des Netzwerks verschaffen und noch größeren Schaden anrichten. EDR wappnet Endgeräte gegen derlei Gefahren – und bei Geräten des hier beschriebenen Benutzertyps ist der Schutz mittels EDR ein Muss.

Sie müssen sich nicht für die eine oder andere Lösung entscheiden, wie bereits gesagt. EDR mag zwar den umfassenderen Schutz bieten, doch wenn ein Kompromiss erforderlich ist, können Sie ihren Einsatz durchaus strategisch abwägen.

Das Kostenargument

Zu einer sachlich fundierten Entscheidung gehört auch die Frage nach den Kosten. Diese liegen bei EDR pro Platz höher als bei herkömmlicher AV – den einen oder anderen Kunden könnten potenzielle Mehrkosten erst einmal abschrecken, vor allem wenn er mit seiner bisherigen Lösung

gut gefahren ist. Doch Cybergefahren und die durch sie verursachten Schäden werden weiter zunehmen und manchen Unternehmen ist vielleicht nicht klar, welcher Gefahr sie tatsächlich ausgesetzt sind und welche Folgen ein Angriff für sie haben könnte. Ein Ransomware-Angriff beispielsweise kann im Nu gesamte Netzwerke lahmlegen und wenn die Infrastruktur komplett neu aufgebaut werden muss, kostet die Behebung des Schadens hier enorm viel Zeit. Allein die Möglichkeit der EDR, derlei Angriffe zu vereiteln, rechtfertigt ihre höheren Kosten vollauf.

Hat Ihr Kunde noch gar keinen Endgeräteschutz, bieten Sie ihm direkt EDR an. Er sollte die Kosten dafür nicht als Mehrkosten für ein Upgrade von AV auf EDR betrachten und durch EDR ein besseres Sicherheitsgefühl haben. Alleine das rechtfertigt die Entscheidung allemal. An dieser Stelle noch ein Wort zu Ihren eigenen Servern: diese schützen Sie am besten genauso wie die Ressourcen, die Sie auf ihnen hosten – durch EDR.

Kunden, die als Argument gegen EDR die Mehrkosten anführen, sollten Sie dezidiert aufzeigen, was sie für ihre Investition gewinnen: Zeit. Ein Geräterollback ist mit EDR in weniger als einer Minute erledigt – ein neues Geräte-Image würde vier bis sechs Stunden dauern. Außerdem erhalten Sie detaillierten Einblick in den Vorfall. So können Sie in ähnlich gelagerten Fällen künftig noch besser reagieren, was Ihre fachliche Kompetenz als Anbieter von Sicherheitsdiensten und Ihre Rolle als zuverlässiger Berater stärkt.

Wenn Sie einem Kunden EDR nicht entschieden genug anbieten, weil normaler AV vielleicht ja auch genügt, riskieren Sie letztlich selbst etwas. Denn die Wahrscheinlichkeit, dass Sie diesen Kunden im Fall einer Datenschutzverletzung verlieren würden, ist hoch. Für Ihre Kunden sind Sie der Experte, der sich um ihre IT- und Sicherheitsprobleme kümmert. Das gilt auch für die preissensibleren unter ihnen, bei denen Sie sich scheuen mögen, EDR anzubieten. Doch dieser Schuss geht eben leicht nach hinten los, wenn ein solcher Kunde dann doch Opfer eines Datendiebstahls wird.

Bei Kunden, die sich um keinen Preis der Welt von EDR überzeugen lassen möchten, belassen Sie es einfach bei einem Schutz durch AV. Letztlich gilt, dass von einem umfassenderen Schutz beide Seiten profitieren – Sie und Ihr Kunde.

Fazit

AV und EDR – beide haben ihre Berechtigung. Angesichts der sich verschärfenden Gefahrensituation und der ständigen Innovation könnte der klassische AV aber durchaus bald Geschichte sein und EDR zum neuen Sicherheitsstandard avancieren. Die Vorteile, die EDR bietet, dürften die für ihren flächendeckenden Einsatz anfallenden Mehrkosten vertretbar machen.

Aber auch wenn die Rollback-Funktion in EDR bei Ransomware helfen kann, ersetzt EDR kein vernünftiges, Cloud-Backup. Die Sicherung von Daten an einem dritten Ort und ein regelmäßiger Test von Backups auf ihre Funktionsfähigkeit sind und bleiben ein wichtiges Element der Cyberhygiene. Davon abgesehen schützen Backups nicht nur vor Ransomware, sondern auch vor Datenverlusten durch Softwarefehler, Hardwareprobleme, versehentliches oder absichtliches Löschen von Daten durch Mitarbeiter oder Naturkatastrophen.

EDR oder Antivirus? Sie haben die Wahl und können beides je nach Kundenbedarf kombinieren. Ganz gleich, wofür Sie sich entscheiden, N-able kann Ihnen helfen.

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