Für alle Sicherheitsvorfälle gerüstet

EDR-Lösungen tragen zur IT-Sicherheit bei, indem sie Bedrohungen an den Endpunkten erkennen, visualisieren und das Ergreifen geeigneter Massnahmen ermöglichen. Ruedi Kubli, Fortinet-Team-Leader beim IT-Security-Distributor BOLL, erklärt im Interview, worum es dabei geht.

Ruedi Kubli ist Fortinet-Team-Leader beim IT-Security-Distributor BOLL.

Wieso braucht es EDR?

Ruedi Kubli: EDR steht für «Endpoint Detection and Response» – also für das Erkennen von Cyberbedrohungen auf den Endgeräten sowie die passende Reaktion darauf. Da der Datenverkehr via Internet meist verschlüsselt abläuft, werden konventionelle Schutzlösungen gewissermassen blind für allfällig enthaltene Malware. Diese tritt erst auf dem Endgerät entschlüsselt ans Licht und wird dort – sofern nicht eingegriffen wird – ausgeführt. Signaturbasierte Antivirus-Lösungen erkennen nur bereits bekannte Schädlinge. Unbekannte Bedrohungen laufen an der AV-Lösung vorbei. Hier kommt EDR ins Spiel.

Wie arbeiten EDR-Lösungen?

EDR basiert auf dem Aufspüren von potenziell schädlichem Verhalten. Dabei kommt Machine Learning zum Zug. So wurde beispielsweise die EDR-Software FortiEDR von Fortinet anhand unzähliger existierender Malware trainiert. Dadurch kann sie erkennen, wenn ein anomales Verhalten zu befürchten ist. Ist dies der Fall, blockiert sie den Verkehr des Clients mit dem Unternehmensnetzwerk, die Nutzung einer bestimmten Anwendung oder das Öffnen des potenziell infizierten Dokuments.

Ist das schon die ganze Zauberei?

Nein. Das automatische Blockieren ist nur der erste Schritt. Man kann ja beispielsweise einen betroffenen Client nicht ewig vom Netz trennen. Aufgrund der Informationen, die das EDR-System als gut verständliche Visualisierung liefert, muss das Unternehmen nun passend reagieren. Dabei sind etwa die folgenden Fragen zu beantworten: Soll der Client von der Malware gesäubert oder komplett neu aufgesetzt werden? Muss man die betroffene Anwendung patchen? Und wie soll das infizierte Dokument gehandhabt werden, damit es sicher geöffnet werden kann und wichtige Informationen für die Analyse liefert. Entscheidungen dieser Art kann eine EDR-Lösung nicht selbst treffen.

Braucht es zur Klärung dieser Fragen nicht umfangreiches Security-Know-how?

Ja, das ist so. Allerdings haben nicht alle Unternehmen die nötigen Ressourcen und Kompetenzen im Haus. Firmen mit einem eigenen Security-Team können sich selbst darum kümmern. Andere jedoch sind auf externe Unterstützung angewiesen. Dabei kann ein Dienstleistungsanbieter mit einem Managed Security Service helfen. Und auch dieser profitiert vom installierten EDR-System – denn eine gute EDR-Lösung muss in der Lage sein, dem Managed Service Provider alle nötigen Informationen zu liefern, damit er zielgerichtet reagieren kann.

Sie leiten bei BOLL das Fortinet-Team. Was bietet Fortinet in Sachen EDR?

EDR ist gewissermassen ein Buzzword der Stunde. Viele Security-Anbieter offerieren eine EDR-Lösung, wobei der Aspekt des «Response» oft untergeht. Die EDR-Plattformen bieten schöne Visualisierungen an und automatisieren via Playbooks die gängigsten Reaktionen auf gefundene Schädlinge. Aber der Rest wird dem Anwender überlassen. Fortinet geht hier einen Schritt weiter: In Ergänzung zu FortiEDR offeriert Fortinet einen Managed Detection and Response Service (MDR), der – kombiniert mit dem FortiGuard Incident Response Service – das Team des Kunden unterstützt. Zusammengefasst sprechen wir von sogenannten «FortiGuard Responder Services».

Was ist darunter zu verstehen?

Diese Dienste bieten den Kunden eine 24/7-Überwachung sowie eine Triage der Warnmeldungen. Zudem unterstützen sie das wirksame Handling der Vorfälle. Dabei kommen sowohl die EDR-Plattform beim Kunden als auch für weitere Analysen die FortiGuard-Plattform bei Fortinet zum Einsatz – und natürlich das reiche Know-how der Fortinet-Experten. Diese untersuchen und analysieren jeden Alert, ergreifen Massnahmen zum Schutz der Kunden und liefern konkrete und detaillierte Empfehlungen zur Problembehebung sowie zu den Folgeschritten, welche die zuständigen Administratoren angehen sollten.

Wie gliedern sich EDR-Lösungen in die restliche IT ein?

EDR-Plattformen sind keine Insellösungen. Sie müssen sich vielmehr mit der Security-Landschaft verzahnen, sodass die Informationen von verschiedenen Systemen genutzt werden können. Wenn EDR eine Bedrohung gefunden hat, sollte dies beispielsweise auch die Firewall wissen. Innerhalb des Security-Portfolios eines Herstellers sind die Lösungen in der Regel gut integriert – zumindest bei Fortinet ist das durchgängig der Fall. In heterogenen Umgebungen müssen Drittherstellerprodukte via API angebunden werden, was Entwicklungsaufwand mit sich bringt.

BOLL
IT Security Distribution

BOLL Engineering AG

Jurastrasse 58
5430 Wettingen
Tel. 056 437 60 60

info@boll.ch
www.boll.ch