Advertorial

Massgeschneiderte Endpoint Security für jeden Bedarf

Bedrohungen aus dem Cyberspace werden immer häufiger und raffinierter. Erkennung und Abwehr von Attacken setzen fortgeschrittene Sicherheitskonzepte wie Endpoint Detection and Response (EDR) voraus – und auch Security-Know-how, das beim Kunden, beim Reseller oder beim Lösungsanbieter angesiedelt sein kann.

Cyberkriminelle entwickeln im Rekordtempo immer wieder neue Viren, Trojaner, Ransomware-Schädlinge sowie andere Malware und nutzen diese für immer raffiniertere und schwieriger zu erkennende Angriffe mit teils katastrophalen Folgen für die betroffenen Unternehmen. Mit Endpoint Detection and Response (EDR) existiert seit einiger Zeit ein Ansatz zur Bekämpfung fortgeschrittener Attacken auf dem Endgerät, der klassischen Endpoint-Security-Lösungen überlegen ist.

Der Durchblick ist allerdings nicht immer einfach, denn EDR-Lösungen finden sich mittlerweile im Programm der meisten Security-Anbieter. Am Beispiel der Lösungspalette von Kaspersky lässt sich zeigen, dass EDR nicht gleich EDR ist – je nach dem Sicherheits-Know-how in der Organisation, den spezifischen Bedürfnissen des Kunden und der Beziehung zwischen Kunde und Security-Partner können unterschiedliche Produkte und Services zum Einsatz kommen.

EDR Optimum: Ideal bei gutem Security-Know-how

Die Kaspersky-Plattform EDR Optimum stützt sich auf den bewährten Unterbau der Endpoint-Schutzlösung Kaspersky Endpoint Security for Business Advanced – oder auf vergleichbare Produkte – und ergänzt diese mit EDR-Funktionalität: Während klassische Endpoint Security Schädlinge entdeckt und blockiert, unterstützt EDR die Security-Verantwortlichen massgeblich dabei, passend und Compliancekonform zu reagieren (Response). Die Lösung ist leicht zu implementieren und stellt, da sie zusammen mit Endpoint Security for Business auf einen einzigen Agenten setzt, für die Endgeräte keine zusätzliche Belastung dar.

Ebenso einfach ist die Lizenzierung. Der Reseller kann für Kunden, die schon Endpoint Security for Business Advanced einsetzen, EDR als Add-on hinzufügen. Wenn noch keine Kaspersky-Produkte im Einsatz stehen, kann der Kunde direkt mit EDR Optimum beginnen und erhält automatisch den Advanced-Unterbau dazu.

EDR Optimum kommt am besten zum Tragen, wenn der Kunde oder sein Partner über gutes Security-Know-how verfügt und die von der Plattform gelieferten Informationen und Reports aktiv in passgenaue Reaktionen umsetzen kann.

Managed Detection and Response: Kaspersky wird aktiv

Mit der cloudbasierten Lösung Managed Detection and Response (MDR) bringt Kaspersky das Wissen seiner Spezialisten direkt an den Reseller beziehungsweise an dessen Kunden: Kaspersky überwacht die Endpunkte, betreibt dabei proaktive Suche nach Bedrohungen (Threat Hunting) und kümmert sich entweder selbst um deren Abwehr oder gibt dem Reseller Anleitung, wie vorzugehen ist (Guided Response). Auch MDR fusst auf dem bekannten Kaspersky-Unterbau.

Bei Kaspersky MDR übergibt der Reseller das Zepter zumindest teilweise an Kaspersky, ohne dabei aber die Kontrolle zu verlieren. Die Lösung eignet sich somit für Reseller mit beschränkten Security-Ressourcen – aber auch für solche mit gutem IT-Sicherheitsverständnis.

XDR: Die Plattform für Experten

Mit seinem Expert Framework und der Anti Targeted Attack Platform (KATA) richtet sich Kaspersky an Reseller, die eigene Security Operation Center (SOC) betreiben und deren tägliches Brot die Cybersecurity ist. Die Lösung erkennt multidimensionale Bedrohungen auf Endpoint- sowie auf Netzwerkebene, verschafft umfassende Transparenz und bietet komplexe Analysen und Abwehrmassnahmen. KATA zielt auf grössere Unternehmen, etwa in Branchen wie Finanzwesen, Energie und Telekommunikation, sowie Behörden.

Mit diesen drei unterschiedlich ausgerichteten Plattformen im EDR-Umfeld bietet Kaspersky ein Mass an Flexibilität, das kaum ein anderer Anbieter offeriert, sowohl hinsichtlich der Möglichkeiten für die verschiedensten Kunden als auch punkto Lizenzierung auf Monats- oder Jahresbasis. Auf Wunsch führt Kaspersky bei den Kunden auch Security-Audits durch – für den Reseller eine Möglichkeit, sein Geschäftsmodell mit einem Security-Compliance-Dienst abzurunden.

- EDR mit Kaspersky: die Vorteile
- EDR-Plattformen passend für jeden Bedarf
- Bewährte Basis mit Endpoint Security for Business
- Einfache Implementation, einfache Lizenzierung
- Umfassende Transparenz, punktgenaue Abwehr
- Geeignet für unterschiedliches Mass an vorhandenem Security-Know-how

Kontakt:

BOLL Engineering AG
Jurastrasse 58, 5430 Wettingen
Tel. 056 437 60 60
info@boll.ch, www.boll.ch