Cybersecurity für KMUs auf Enterprise-Niveau

Der Cybersecurity-Anbieter WatchGuard bleibt seinem KMU-Fokus treu und ermöglicht mit Lösungen wie WatchGuard MDR und ThreatSync+ NDR kleinen und mittleren Unternehmen ein Niveau an Cybersicherheit, das sich bisher nur Grossunternehmen leisten konnten. Bernhard Aregger von BOLL Engineering erklärt, wie das geht.

BOLL und WatchGuard arbeiten seit über 30 Jahren zusammen. Wie hat sich WatchGuard in dieser Zeit entwickelt?
Bernhard Aregger: Die rote WatchGuard-Firebox war die erste Firewall-Appliance, die das Netzwerk zu erschwinglichen Kosten absicherte. Diesem Grundsatz ist WatchGuard stets treu geblieben und deckt heute mit der Unified Security Platform die kompletten Cybersecurity-Ansprüche von KMUs, dezentral organisierten Unternehmen und Anbietern von Managed Security, sogenannten Managed Security Providern (MSP), ab. WatchGuard eignet sich nicht zuletzt deshalb perfekt für den KMU-geprägten Schweizer Markt.

Entwickelt hat sich auch die Bedrohungslage. Welche Probleme sind heute besonders aktuell?
Zunächst sicher die schiere Masse an neuen, immer raffinierteren Bedrohungen. Es finden ständig erfolgreiche Angriffe auch auf bestens gesicherte Netzwerke statt. Dies nicht zuletzt dadurch, dass Angreifer zunehmend künstliche Intelligenz für ihre Attacken nutzen. So sind zum Beispiel gefälschte, zwecks Phishing versendete E-Mails immer schwieriger als solche zu erkennen. Zweitens vergehen zwischen dem eigentlichen Angriff und der Erkennung sowie getroffenen Gegenmassnahmen oft Wochen bis Monate.

Wie geht WatchGuard mit diesen Bedrohungen um?
Der Ansatz von WatchGuard ist es, einen Angreifer so früh wie möglich zu erkennen, ihn zu isolieren und das Problem so schnell wie möglich zu eliminieren. Neben den klassischen Hardware-Appliances kommen dazu neue Technologien wie die WatchGuard Cloud sowie Dienste wie Managed Detection and Response (WatchGuard MDR) und Network Detection and Response (ThreatSync+ NDR) zum Einsatz. Diese Services ermöglichen es Partnern, ihren Kunden umfassende Cybersicherheitsdienste anzubieten.

Worum geht es bei WatchGuard MDR?
Den meisten KMUs fehlen Zeit und Ressourcen, um die Cybersicherheit in den Griff zu bekommen. Sie lagern diese deshalb vermehrt an Managed Security Provider (MSP) aus. Doch auch diese verfügen selbst oft nicht über das Personal und das Investitionsvolumen für den Betrieb eines Security Operations Center (SOC), das rund um die Uhr reibungslos seine Leistung erbringt. Mit dem MDR-Service bietet WatchGuard den Partnern proaktive Cybersicherheit an: Ein qualifiziertes Team von Cybersicherheitsexperten schützt die Endpunkte der Kunden mit 24/7-Überwachung, Threat Hunting sowie Erkennung, Abwehr und Eindämmung von Angriffen.

Bernhard Aregger ist Sales Specialist bei BOLL.

Und was ist ThreatSync+ NDR?
Dabei handelt es sich um eine hundertprozentig cloudbasierte, KI-gesteuerte Lösung für Threat Detection and Response mit offenem Netzwerk mit unternehmensweiter Netzwerküberwachung, Erkennung und Reaktion. Sie erkennt unter anderem Ransomware und Angriffe auf Lieferketten, deckt versteckte Netzwerkrisiken auf und reduziert die Erkennungszeiten auf Minuten. Dazu nutzt ThreatSync+ NDR eine der modernsten KI-Engines mit mehrstufigem neuronalem Netzwerk, erkennt und korreliert Anomalien und findet damit auch intern bedingte Netzwerkrisiken. Darüber hinaus unterstützt die Lösung mit optionalem Compliance Reporting auch dabei, die NIS2-Vorgaben der EU einzuhalten. Unterstützt wird zudem die internationale Norm ISO 27001.

Was sind die Vorteile der NDR-Lösung von WatchGuard?
Sie ist ganz auf die Bedürfnisse von KMUs ausgelegt, im Gegensatz zu herkömmlichen NDR-Lösungen, die ein aufwendiges SOC voraussetzen. Sie arbeitet in der WatchGuard Cloud und macht neue Hardware für den Betrieb der NDR-Funktionalität überflüssig. Das Allerwichtigste ist jedoch, dass ThreatSync+ NDR die Ergebnisse auf einem intuitiven Dashboard präsentiert, das konkrete Rückschlüsse auf Vorfälle, betroffene Geräte und Benutzer sowie die zeitliche Abfolge liefert, sodass sich Partner und Kunden auf die kritischsten Risiken konzentrieren können. Kurz gesagt: ThreatSync+ NDR bietet für KMUs leicht verständliche SOC-Funktionen auf Enterprise-Niveau ohne hohe Personal- und Betriebskosten.

BOLL
IT Security Distribution

BOLL Engineering AG

Jurastrasse 58 | 5430 Wettingen
Tel. 056 437 60 60 | info@boll.ch
www.boll.ch