10 JAHRE
2010 – 2020
IT-MARKT

«IT-Security wurde vor zehn Jahren zum zentralen Baustein»

Vor über 30 Jahren hat Thomas Boll den heutigen VAD Boll Engineering gegründet. Während der 90er-Jahre verlagerte sich der Fokus des Unternehmens von der Softwareentwicklung auf IT-Security. Im Interview blickt der CEO zurück auf das vergangene Jahrzehnt, sagt, wie sich die Branche veränderte und wohin die Reise noch führen wird. Interview: Coen Kaat

«Der Channel tut sich oft schwer mit der Beurteilung, welche neuen Technologien sich durchsetzen werden»

Thomas Boll, CEO, Boll Engineering

Wie sah der IT-Security-Channel vor zehn Jahren aus?
Thomas Boll: Unsere Reseller waren in puncto IT-Security vor allem damit beschäftigt, die Unternehmensnetzwerke ihrer Kunden vom Internet abzuschotten, beziehungsweise zu schützen. Das dominante Buzzword dieser Zeit lautete «Perimeterschutz». Die IT-Security wurde vor zehn Jahren definitiv zum zentralen Baustein einer sicheren Netzanbindung. Gleichzeitig entwickelte sich ein klarer Trend hin zur Zentralisierung der Sicherheit. Dazu wurden komplementär Aufgaben in konsolidierenden Appliances zusammengeführt. Diese mit Unified Threat Management und etwas später dann mit Next Generation Firewall bezeichneten Systeme bildeten für mehrere Jahre das Rückgrat einer integralen Data Center Security beziehungsweise einer effizienten Abwehr von Cybergefahren.

Was war Ihrer Meinung nach die einschneidendste Veränderung in dieser Zeit?
Die IT-Security-Lösungen sind umfassender und komplexer geworden. Dies führt zu gesteigerten Beratungs-, Wartungs- und Support-Aufwendungen, erfordert ein hohes Mass an Know-how und bedingt hochgradig versierte Spezialisten. Zudem hat sich das User-Verhalten stark verändert. Mobile Arbeitsplätze oder die Nutzung von Cloud-Diensten beispielsweise verschaffen der Client- und Cloud-Security eine wachsende Bedeutung. Hinzu kommt, dass Hersteller vermehrt neue Produkte auf den Markt werfen, was die Konkurrenzsituation verstärkt. Allerdings sind neue Abwehrdispositive – zum Beispiel Lösungen, die Angriffsmuster generisch erkennen – notwendig, um der extremen Datenflut und den zahlreichen, hocheffizienten und noch unbekannten Angriffsvektoren Herr zu werden. Dabei tut sich der Channel oft schwer mit der Beurteilung, welche der neuen Technologien und Produkte sich durchsetzen werden. Zudem fehlen die notwendigen Ressourcen, um neue Produkte ins Portfolio zu integrieren.

Was sollte sich jetzt Ihrer Meinung nach idealerweise noch ändern?
Um langfristig erfolgreich zu sein, sind aus meiner Sicht loyale, langjährige und von Vertrauen geprägte Partnerschaften zwischen Herstellern, Distributoren und Resellern notwendig. Nur so kann es sich für die Channelpartner lohnen, etwa in den Aufbau eines neuen Brands zu investieren. Zudem müssen sich Distis zu IT-Firmen wandeln, um den Herausforderungen und den Bedürfnissen des Marktes zu entsprechen. Reine Box-Mover haben ausgedient.

In welche Richtung bewegt sich der Markt zurzeit?
Aus technischer Sicht sind dies Themen wie Cloud-Security, das Zusammenwachsen sich ergänzender Sicherheitsmassnahmen, die dezentrale Nutzung von Daten aus dem Client-Netzwerk und der Cloud sowie ein übergreifendes IT-Security-Management. Zur grossen Herausforderung für den Channel aber wird die Umsetzung neuer Geschäftsmodelle – dies vor dem Hintergrund, dass Kunden vermehrt Lizenzen direkt aus der Cloud beziehen und Hersteller ihre Kunden vermehrt direkt bedienen. Angesichts dessen muss der Channelpartner anderweitig Mehrwert schaffen – etwa durch die Positionierung als Managed Security Service Provider, bei dem Produkte integrale Bestandteile des Lösungsangebots sind. Diese Abkoppelung vom Produktverkauf generiert einen kontinuierlichen «Revenue Stream» und lässt sich gut skalieren.

Das vollständige Interview finden Sie online
www.it-markt.ch