ICTkommunikation im Gespräch mit Thomas Boll, CEO Boll Engineering

«Der Schutz von Hardware, Software und Unternehmen ist eine zentrale und immer anspruchsvoller werdende Herausforderung.»

In der IT-Security herrscht ein permanenter Druck zur Erneuerung

Laut Thomas Boll, CEO der auf IT-Security fokussierten Wettinger Value-Added-Distributorin Boll Engineering, stellt das Management von IT-Security ein starkes Thema im Bereicht der IT-Sicherheit dar. Auf welche weitere Schwerpunkte und kommende Trends sich die Schweizer Unternehmen einstellen müssen und wie sich ein Distributor auf die ständig komplexer werdenden Herausforderungen der Sicherheit einstellt, verrät er im Interview des Monats.

Von Karlheinz Pichler (Interview) und Susanne Seiler (Fotos)

Noch vor vier, fünf Jahren stand das Thema «IT-Security» ganz zuoberst auf den Agenden der CIOs. Mittlerweile sind es die Anwendungsmöglichkeiten der Informationstechnik selbst, die sich in den Vordergrund geschoben haben – Stichwörter: Cloud Computing, Soziale Netze, «Bring your own Device» (Byod) etc. Dies aber sind wiederum exakt IT-Bereiche, bei denen wohl gar nichts ginge, stünde nicht die IT-Sicherheit als quasi Schutzengel dahinter. Für Sie als Chef einer Value-Added-Distributionsfirma, die auf IT-Sicherheit fokussiert ist, müsste aus ökonomischer Sicht also eigentlich alles eitle Wonne sein. Ist dies denn auch so?

Es ist in der Tat so: Die IT-Security ist oft nicht im Fokus der Aufmerksamkeit. Trotzdem ist und bleibt sie ein Kernthema im Bereich der Informationstechnologie. Ob im Datencenter oder beim Kunden selbst – der Schutz von Hardware, Software und Unternehmen ist eine zentrale und immer anspruchsvoller werdende Herausforderung. Dazu tragen auch neue, sich verändernde Themen bzw. Gefahren bei. So zum Beispiel die zunehmende Mobilität – Stichwort: «Bring your own Device» –, der markante Auf- und Ausbau von WLANs oder die enorme Nutzung von Social-Media-Plattformen. Letztgenannte etwa führen dazu, dass Inhalte und Funktionen individuell gefiltert oder blockiert und dass Gefahren frühzeitig erkannt werden müssen.

Die Nachfrage nach IT-Security-Produkten ist zwar ungebrochen. Doch diesem positiven Trend entgegengesetzt ist die Tatsache, dass die finanziellen Ressourcen der Kunden begrenzt sind und dass folglich eine Allokation der benötigten Mittel nicht immer im erforderlichen Mass möglich ist. Dies verursacht einen zunehmenden Druck auf die Kosteneffizienz. Feststellbar ist ferner, dass kommerziell interessante Themen von zahlreichen Herstellern angegangen werden und dass diese vermehrt Lösungen mit überlappenden Features auf den Markt bringen. Alleinstellungsmerkmale zu finden wird deshalb immer schwieriger und Security-Produkte werden mehr und mehr zur Commodity. Vor diesem Hintergrund erstaunt es nicht, dass anbieterseitig alle Marktteilnehmer einem steigenden Preis- und Konkurrenzdruck ausgesetzt sind.

ZUR PERSON

Der Eigentümer und Geschäftsführer der Boll Engineering AG, Thomas Boll, wurde 1959 geboren und wohnt heute im aargauischen Baden. Nach seiner Ausbildung zum Dipl. El. Ing. ETH war er zunächst in der Software-Entwicklung als Consultant im Enterprise-Umfeld tätig. Im Jahre 1988 gründete er die Security-Spezialistin Boll Engineering AG, deren Geschäftsführer er heute noch ist. Thomas Boll stand auch während sieben Jahren als Präsident dem Verband / ch/open als Präsident vor.

Antivirensoftware oder Firewalls haben heute wohl bereits so ziemlich alle Firmenanwender verinnerlicht. In welchen Bereichen spüren Sie derzeit die grösste Nachfrage?

Wir sind stark im Bereich Perimeter-Security tätig, in einem Umfeld also, das nichts an Wichtigkeit eingebüsst hat. Einerseits spüren wir einen zunehmenden Bedarf an Datacenter-Firewalls – sowohl von Service-Providern als auch von Enterprise-Kunden, die externe Datacenter benutzen. Es werden vermehrt Datenraten von 10 Gbit gefordert. Andererseits besteht ein kontinuierlicher Erneuerungsdruck, der unter anderem durch höhere Bandbreiten, neue Bedrohungen wie «Modern Malware» sowie leistungsfähigere Technologien forciert wird. IT-Security-Systeme müssen in der Regel innert weniger Jahre ersetzt werden. Andererseits führt die Integration zusätzlicher Security-Funktionen in ein und dieselbe Appliance dazu, dass Kunden vermehrt neue Lösungen beschaffen. Auslöser dazu sind beispielsweise die Einbindung von Funktionen wie VPN, SSLVPN und Content-Filter in eine universelle UTM-Appliance.
Etwas schwerer tun sich neue, innovative Produkte wie beispielsweise Secure-E-Mail-Lösungen bzw. Appliances zur digitalen Signatur und Verschlüsselung von E-Mails. Dies vor allem deshalb, weil Firmen vorrangig ihre Basis-Security sicherstellen und sich erst in zweiter Linie mit ergänzenden, vermeintlich nicht zwingend notwendigen Sicherheitsvorkehrungen auseinandersetzen. Security-Lösungen, die sich nicht als «Best Practice» etabliert haben, fallen oft durchs Netz der Investitionen.

Wo sehen Sie selber mittel- und längerfristig die grössten Herausforderungen im Bereich der IT-Sicherheit?

Ein grosses Thema ist die Managebarkeit der IT-Security. Dank leistungsfähigen Systemen haben wir beispielsweise die Möglichkeit, höchst granulare Einstellungen vorzunehmen und etwa Social-Media-Anwendungen individuell freizugeben. Dies setzt aber übersichtliche, einfach bedienbare Management-Systeme voraus.
Ein ähnliches Bild präsentiert sich in Bereichen wie Alarmierung, Logging oder verhaltensbasierten Analysen. Moderne Systeme sind in der Lage, unendlich viele Informationen aufzubereiten. Doch wie gehen die Verantwortlichen mit der schier unendlichen Datenmenge um? Sind sie überhaupt in der Lage, alle relevanten Informationen als solche zu erkennen und

ZUR FIRMA

Die Boll Engineering AG ist im Jahre 1988 in Wettingen gegründet worden. Das Unternehmen ist ein «Full Service Master Distributor» für IT-Security- und Internet-Access-Lösungen. Das ganzheitliche Angebot adressiert die Bereiche Netzwerk-Security, Mail-Security, Identity und Access Management, Secure Internet Access sowie Internet und Server Load Balancing. Darüber hinaus bietet Boll Engineering auch ein breites Schulungs- und Trainingsangebot mit entsprechenden Zertifizierungen an.

die gegebenenfalls Tausenden von Warnungen richtig zu interpretieren? Trends wie Mobile Computing und Virtualisierung machen die Sache auch nicht einfacher. Kurz: Es wird immer schwieriger, zu sehen, was im Netz passiert. Neue Lösungen hinsichtlich Aufbereitung der Daten sind folglich nötig. IT-Security-Verantwortliche benötigen starke Werkzeuge, um zu sehen, wo Handlungsbedarf besteht. In diesem Bereich besteht für die Lösungsanbieter noch ein grosses Entwicklungspotenzial.

Ihr Unternehmen wird nächstes Jahr 25 Jahre alt. In diesen Jahren hat es sich von einer Software-Schmiede zu einem Distributionsunternehmen gewandelt. Was hat diesen Wandel bewirkt? Wird bei Boll Engineering heute noch in irgendeiner Form Entwicklungsarbeit geleistet?

In den ersten Jahren unseres Bestehens waren wir ein Software entwickelndes Unternehmen mit einem starken Fokus auf technisch orientierte Projekte im Kommunikationsbereich. Wir haben uns also schon damals stark mit Themen wie Networking und Security auseinandergesetzt. Um im Entwicklungsbereich jedoch langfristig eine wichtige Rolle zu spielen, hätten wir uns zur grossen Software-Schmiede entwickeln müssen – und das war nicht unser Bestreben. Deshalb haben wir uns gezielt auf den Bereich der IT-Security fokussiert und uns im «2-Tier»-Modell auf die Rolle des VADs, des Value Added Distributors konzentriert. Dies ermöglicht uns einerseits eine enge Zusammenarbeit mit den Herstellern. Andererseits haben wir damit Rahmenbedingungen geschaffen, um uns auch langfristig durch Engineering-Kompetenzen und einen klaren Technik-Fokus am Markt zu behaupten. Auch heute ist die Begeisterung für die Technik bei all unseren Mitarbeitenden spür- und sichtbar. Und so erstaunt es nicht, dass wir uns nicht primär über den eigentlichen Warenhandel selbst, sondern über Know-how und «Value Add» definieren.

Ergänzen möchte ich, dass wir auch heute noch Entwicklungsarbeit leisten. So entwickeln wir Tools und Adaptionen, die das Leben unserer Reseller und deren Endkunden einfacher machen. Mit Autodoc beispielsweise haben wir eine Software entwickelt, die aus Firewall-Konfigurationsdateien automatisch ausführliche Reports erstellt. Unser jüngstes Kind ist Fopmap, eine dedizierte Software, die das Roll-out von Firewall-Grossprojekten massiv vereinfacht.

Sie haben heuer ein Distributionsabkommen mit der auf DDoS-Defense (Distributed Denial of Services) fokussierten US-amerikanischen Corero Network Security unterzeichnet. Wie hoch ist denn in der Schweiz für ein Unternehmen generell die Gefahr, von einem DDoS-Angriff getroffen zu werden?

Auch Schweizer Organisationen und Firmen sind vor DDoS- und vergleichbaren Attacken nicht verschont, wie dies die Angriffe auf Postfinance im Zusammenhang mit Wikileaks deutlich machen. Nachdem die Schweizer Post das Konto von Wikileaks geschlossen hatte, geriet das Postfinance-Webportal unter Beschuss von Hackern und war dadurch zeitweise nicht mehr erreichbar. Zu beachten ist, dass nur ein Bruchteil der ausgeführten DDoS-Angriffe überhaupt bekannt wird, da Firmen verheimlichen, Opfer einer Attacke geworden zu sein. Es muss mit einer hohen Dunkelziffer gerechnet werden.

DDoS-Attacken sind in der Regel das Werk von verteilten, meist anonymen, nicht fassbaren Gruppierungen wie beispielsweise Anonymus. Sie sind häufig politisch motiviert. Doch auch DDoS-Attacken aus kommerziellen Gründen sind nach wie vor existent. Speziell gefährdet sind Firmen, die direkt vom Online-Handel leben.

Um DDoS-Attacken abzuwehren, gilt es, guten von schlechtem Traffic zu trennen und den Betrieb aufrechtzuerhalten. Das ist allerdings nicht ganz einfach, da Angreifer mit grossem kreativem Potenzial dafür sorgen, dass sich schadhafter Traffic wie legitimer Datenverkehr präsentiert. Zu berücksichtigen ist auch, dass DDoS-Angriffe vermehrt auf Applikationsebene stattfinden. Bei diesen werden seitens der Angreifer nur wenige Ressourcen benötigt. Es werden ganz einfach Software-Schwachstellen ausgenutzt, um das Zielsystem zum Stillstand zu bringen. Klassische Firewalls bzw. UTM-Appliances, die vermehrt auch Content Security-Disziplinen wie Ap-

plication Control, Webfilter und Antivirus in einem System beinhalten, sind nicht in der Lage, einen wirksamen DDoS-Schutz zu bieten. Dies namentlich aus Ressourcengründen. Für den wirksamen Schutz vor DDoS-Attacken müssen dedizierte Appliance eingesetzt werden. Diese werden vor der Firewall eingebunden, um diese vor Überlast zu schützen. Kernaufgabe entsprechender Systeme jedoch ist der wirksame Schutz der Endsysteme.

Vom IT-Security-Portfolio her gesehen ist Ihr Unternehmen sehr breit aufgestellt. Gibt es hier kein Konfliktpotenzial mit den Herstellern, wenn sich etwa Lösungen überschneiden?

Es ist nicht von der Hand zu weisen: Alle Hersteller wollen möglichst breit aufgestellt sein, was zur Überschneidung der Produkte führt. Mit dieser Situation sind wir primär im Firewall-Bereich konfrontiert, wobei sich dies in der Praxis als unproblematisch erweist. Gründe dafür sind einerseits die klare interne Trennung der Kanäle. So sind bei uns unterschiedliche Personen für Verkauf und Support der konkurrierenden Brands zuständig. Andererseits entscheiden sich die Reseller bewusst für einen bestimmten Hersteller und sind diesem gegenüber «committet». Sie investieren in Ausbildung und Zertifizierung, gewinnen Erfahrungen und betreuen eine immer grösser werdende Basis installierter Produkte eines bestimmten Herstellers. Wechselkäufer sind selten.

Was zeichnet die Distributorin Boll Engineering gegenüber anderen aus? Mit welchen Benefits reizen Sie Ihre Reseller zu Höchstleistungen?

Wie bereits erwähnt, haben wir einen starken technischen Background und ausgesprochen erfahrene, kompetente Mitarbeitende. Zudem fokussieren wir uns nicht nur primär auf den Verkauf von Produkten, sondern auf das Erarbeiten und Anbieten von Lösungen. Damit stärken wir unseren Partnern den Rücken.

Generell kann man sagen: Wir sind bestrebt, unseren Resellern alles Notwendige in die Hand zu geben, damit sich diese auf ihre Kunden konzentrieren und ihren Markt möglichst effizient und erfolgreich bedienen können. Dazu bieten wir dem Channel eine breite Palette an Pre- und Post-Sales-Services an. So etwa Schulungen, kostenlose Teststellungen, Marketing-Unterstützung, kostenlosen technischen Support und vieles mehr.

Stichwort Schulung: Boll Engineering zählt ja zu den wenigen Distributoren, die herstellerspezifische Schulungen anbieten. Wurde diese Ausbildungsschiene aufgrund einer inneren Notwendigkeit entwickelt oder durch den Druck der Hersteller?

Zu Beginn unserer Distributionstätigkeit war eine innere Notwendigkeit gegeben, denn herstellerspezifische Schulungen wurden ausschliesslich in den USA angeboten. Wir aber wollten unseren Partnern massgeschneiderte, nähere und folglich auch preiswertere Trainings ermöglichen. Heute sind wir über den Aufbau unseres eigenen ATCs – das Kürzel steht für «Authorized Training Center» – sehr glücklich. Er

hat dazu geführt, dass unsere Partner bestens ausgebildet sind, was die Zusammenarbeit einfacher, effizienter, professioneller gestaltet.
Im Laufe der letzten Jahre hat sich auch ein verstärkter Druck der Hersteller bemerkbar gemacht. Sie fordern vom Kanal den Besuch zertifizierter Ausbildungen, um einen bestimmten Partnerstatus zu erhalten. Dank unserem etablierten ATC sind wir auch diesbezüglich gut aufgestellt.

Von wem genau werden diese Schulungen besucht – nur von den Channel-Partnern oder auch von Anwenderunternehmen?

Grundsätzlich ist unser ATC für jedermann offen. Es liegt jedoch in der Natur der Sache, dass unsere Schulungen primär von Channel-Partnern besucht werden. Aber auch ambitionierte End-User, die beispielsweise für das Gerätemanagement verantwortlich zeichnen, sind immer wieder in unseren Kursen anzutreffen.

Wirft dieser Schulungsbereich etwas für Ihr Unternehmen ab oder muss er querfinanziert werden?

Obwohl unser ATC selbsttragend ist, steht nicht die Profitabilität im Vordergrund. Vielmehr betrachten wir es als notwendig, unseren Kunden auch in diesem Bereich hochstehende Dienstleistungen anzubieten. Das stärkt die Position unserer Reseller – und unsere Position als Mehrwert schaffender Partner.

Ist Boll Engineering auch berechtigt, entsprechende Zertifikate auszustellen?

Ja, wir sind von Zertifizierungsunternehmen geprüft, zertifiziert und dadurch berechtigt, selbst Zertifikate auszustellen.
Die Voraussetzungen zur Vergabe von Ausbildungszertifikaten sind von Hersteller zu Hersteller verschieden. Einige Lieferanten prüfen unser Training Center in eigener Regie. Andere wiederum nehmen dazu die Dienste etablierter Zertifizierungsanbieter wie «Pearson VUE» und «Kryterion» in Anspruch. Diese weltweit tätigen Zertifizierungsanbieter geben uns vor, wie unser Training Center ausgestaltet sein muss. Sie machen Vorgaben zum administrativen Ablauf und zu den Räumlichkeiten, überprüfen in regelmässigen Abständen die Kompetenz unserer Schulungskräfte und sie definieren, wie, wann, wo und mit welchen Mitteln Prüfungen durchgeführt werden müssen. Unser ATC wird folglich regelmässig auf Herz und Nieren geprüft – und bei entsprechender Abnahme zertifiziert.

Die Security-Lösungen werden immer komplizierter und komplexer. Wie halten Sie und Ihr Unternehmen sich selber auf dem neusten Wissensstand?

Einerseits werden wir regelmässig von unseren Herstellern über neue Technologien, Produkte und Features informiert. Andererseits besuchen unsere Mitarbeitenden die angebotenen Schulungen der Lieferanten. Ebenso wichtig ist, dass unsere Technikerinnen und Techniker die vom eigenen ATC angebotenen Trainings und Zertifikatsprüfungen durchlaufen. Und last, but not least: Wir lernen «on the job». So trägt jeder Support-Call und die entsprechende Auseinandersetzung mit der Thematik zu einer Ausweitung von Know-how und Erfahrung bei.

Einer neuen Studie zufolge ist die Schweiz punkto Malware das sicherste aller Länder. Ist dies ein Verdienst von Boll Engineering?

(Lacht) Es ist nicht angemessen, dieses Resultat als Verdienst von Boll zu interpretieren. Wir sind lediglich einer von mehreren Playern, die einen Beitrag zur wirksamen Abwehr von Malware leisten. Wir sind auch zukünftig bestrebt, mit einer innovativen Produkte-Strategie, mit leistungsfähigen Systemen und weitreichenden Dienstleistungen einen Beitrag zur Verbesserung der IT-Security zu leisten – gemeinsam mit unseren Resellern. □