Moneycab Interview

Thomas Boll, CEO BOLL Engineering AG, im Interview

Thomas Boll, CEO BOLL Engineering AG (Bild: BOLL, Moneycab)

20. Januar 2025

Von Helmuth Fuchs

Moneycab: Herr Boll, Ihr Unternehmen ist in der Schweiz, in Deutschland und in Österreich vertreten. Welche Unterschiede gibt es in Bezug auf die ICT-Bedrohungslage oder die Beantwortung der Risiken in den unterschiedlichen Ländern?

Thomas Boll: ICT-Bedrohungen kommen ja meist aus dem Internet, und dieses ist international. Die Angriffe sind die gleichen, die Probleme sind die gleichen, die Gesetzeslage ist vergleichbar, die Sicherheitsnormen sind identisch. Die Bedrohungslage ist somit sehr ähnlich in den drei Ländern. Was nicht unbedingt gleich ist, ist die Marktsituation: Österreich ist ein typisches KMU-Land, Deutschland hat auch sehr grosse Unternehmen, die Schweiz liegt in der Mitte mit vielen KMU, aber auch mit internationalen Konzernen.

> ***«Wir stehen hier noch ganz am Anfang einer grossen Welle beim Thema KI. Es ist deshalb schwierig, den künftigen Einfluss von KI auf die IT und den Einfluss auf die Security einzuschätzen.»*** *Thomas Boll, CEO BOLL Engineering AG*

Wie bewerten Sie die Effektivität traditioneller Sicherheitsmassnahmen im Vergleich zu KI-gestützten Lösungen angesichts der zunehmenden Raffinesse von Cyberangriffen? Welche

spezifischen KI-Technologien setzt BOLL ein?

Wir stehen hier noch ganz am Anfang einer grossen Welle beim Thema KI. Es ist deshalb schwierig, den künftigen Einfluss von KI auf die IT und den Einfluss auf die Security einzuschätzen. Wir gehen aber davon aus, dass der Einfluss sehr gross sein wird. Tatsache ist, dass die Cyberkriminellen KI bereits nutzen, um möglichst schnell möglichst viele Variationen eines Schadcodes in ihre Malware zu integrieren und so manuell kontrollierte Systeme durcheinanderzubringen. Deshalb braucht es auch in der Abwehr KI. Das Volumen der Malware und der Angriffsmuster ist so enorm, dass man es manuell nicht mehr bewältigen kann. Alle Cybersecurity-Anbieter bauen heute KI-Elemente in ihre Lösungen ein, in mehr oder weniger grossem Umfang.

Wie adressieren Sie die Herausforderung der «Supply Chain Attacks», bei denen Angreifer über vertrauenswürdige Drittanbieter in Systeme eindringen? Und welche Strategien empfehlen Sie Unternehmen zur Risikominimierung?

Hier muss man überlegen, inwieweit es Sinn ergibt, Netzwerke applikatorisch zu verbinden. Wenn man die Systeme via APIs und andere Methoden direkt koppelt, entsteht eine enge Verbindung – für den Handel effizient, aber es birgt die Gefahr, dass Sicherheitsprobleme von einem System ins andere verschleppt werden. Vorkehrungen bei APIs und Datenaustausch sind somit zwingend, am besten auf Basis eines Zero-Trust-Konzepts: Es werden so wenig Verbindungen geöffnet wie möglich und nur so wenig Daten wie unbedingt nötig ausgetauscht. Dabei sollten nicht nur sämtliche Zugriffe kontrolliert und überwacht werden, sondern man muss auch die eigenen Datenbestände auf Sicherheit testen.

Wie sieht Ihre Vision für ein sicheres IoT-Ökosystem aus mit der exponentiellen Zunahme von IoT-Geräten? Welche technischen und regulatorischen Änderungen sind Ihrer Meinung nach notwendig?

Es wird uns in Zukunft immer mehr beschäftigen, alle Geräte so zu schützen, dass es nicht zu katastrophalen Ausfallszenarien kommen kann. Ein Problem von IoT-Geräten ist, dass sie breitflächig verteilt sind, ein anderes, dass es sich häufig um kleine Systeme handelt, die man nicht mit Sicherheitssoftware ausstatten kann. Zudem ist die IoT-Landschaft über Jahre und Jahrzehnte organisch gewachsen und nutzt eine grosse Zahl unterschiedlicher Protokolle und Normen.

> ***«Quantenkryptografie ist zunächst eine Katastrophe für die Sicherheit. Sämtliche bestehenden Verschlüsselungslösungen werden sich mit einem funktionierenden Quantencomputer in kürzester Zeit aushebeln lassen.»***

Um dem beizukommen, gibt es verschiedene Ansätze. Spannend finde ich zum Beispiel den Immunity-Ansatz von Kaspersky: Man baut ein Gerät, das a priori sicher ist und dadurch

nicht weiter geschützt werden muss. Weiter ist es wichtig, ein Inventar aller Geräte im Netz zu führen und das Netz bedarfs- und sicherheitsgerecht zu segmentieren. Und falls ein Gerät selbst nicht aktualisiert werden kann, lässt es sich über sogenanntes Virtual Patching mit aktuellen Sicherheitsupdates schützen. Regulatorisch lässt sich wohl nicht mehr ausrichten als die Verantwortung über IoT- und OT-Systeme denjenigen zu übertragen, die sie betreiben.

Inwiefern sehen Sie Quantenkryptografie als potenzielle Lösung für die Sicherheitsherausforderungen im IoT-Bereich? Arbeitet BOLL Engineering an Implementierungen in diesem Bereich?

Quantenkryptografie ist zunächst eine Katastrophe für die Sicherheit. Sämtliche bestehenden Verschlüsselungslösungen werden sich mit einem funktionierenden Quantencomputer in kürzester Zeit aushebeln lassen. Die ganze Industrie basiert auf solchen Verschlüsselungstechnologien. BOLL arbeitet nicht an quantenbasierten Technologien und Implementierungen - beides ist momentan noch Sache der Wissenschaft.

Backdoors in Verschlüsselungssystemen ist eine Debatte, die auch politisch heftig geführt wird: Wo sehen Sie die Balance zwischen nationaler Sicherheit und Privatsphäre der Nutzer? Welche technischen Lösungen schlagen Sie vor?

Backdoors existieren, das ist nachgewiesen. Die Balance zwischen nationaler Sicherheit und Privatsphäre ist absolut entscheidend. Auch kleinere Organisationen und Einzelpersonen müssen das Recht haben, Daten sicher auszutauschen. Wenn es um terroristische Aktivitäten geht, muss der Staat eingreifen können. Aber wo setzt man die Grenze? Es soll auf alle Fälle immer um Sicherheit gehen und nicht um Missbrauch des Möglichen.

Wie bewerten Sie die Sicherheit und Privatsphäre dezentraler Messaging-Protokolle im Vergleich zu zentralisierten Diensten? Welche Lösungen bietet BOLL Engineering in diesem Bereich?

Dezentrale Protokolle lösen ein wichtiges Problem zentral organisierter Messaging-Dienste: Mit zentralen Servern erhält der Betreiber potenziell Zugriff auf die übermittelten Nachrichten. Es ist immer ein Trade-off: Hat man wie im Darknet absolute Privatsphäre, oder zieht man so vor allem Kriminalität an? BOLL arbeitet jedoch nicht an diesem Thema, wir schützen Kunden vor Angriffen und Daten vor Entwendung. Kommunikationslösungen bieten wir nicht an.

Welche Rolle spielen Software-Defined Networking (SDN) und Network Function Virtualization (NFV) in Ihren Netzwerk-Sicherheitslösungen? Wie integrieren Sie diese Technologien mit traditionellen Sicherheitsmassnahmen?

Hier ist die Cybersecurity-Industrie schon einen Schritt weiter, wir sprechen heute von SASE und ähnlichen Technologien. In der IT gibt es einen grundsätzlichen Virtualisierungstrend. Alles, was früher hardwarebasiert ablief, lässt sich weitgehend virtualisieren. Mit der Virtualisierung von Netzwerken kann die Komplexität deutlich reduziert werden, zum Beispiel für Unternehmen mit vielen verteilten Standorten. Unser Portfolio enthält viele Lösungen in diesem Bereich, von Anbietern, die nur sichere Netzwerkvirtualisierung im Programm haben, bis zu solchen mit integrierten Lösungen, die Netzwerkvirtualisierung und umfassende Sicherheit kombinieren.

> ***«Mit der Virtualisierung von Netzwerken kann die Komplexität deutlich reduziert werden, zum Beispiel für Unternehmen mit vielen verteilten Standorten.»***

Die wachsende Beliebtheit hybrider Cloud-Lösungen bringt eine erhöhte Komplexität und damit auch neue Risikofaktoren mit sich. Welche spezifischen Herausforderungen sehen Sie für die Netzwerksicherheit?

Wer nur auf einen Cloud-Anbieter setzt, ist von diesem vollständig abhängig. Hybride Cloud-Lösungen beheben dieses Problem. Auf der anderen Seite werden Systeme aus Kostengründen wieder vermehrt als On-Premises-Lösung migriert. Für das Problem der steigenden Komplexität der hybriden Cloud haben wir als Sicherheitsspezialisten Multi-Cloud-fähige Lösungen, die nicht auf einen bestimmten Cloud-Provider aufsetzen, sondern für homogene Sicherheit über mehrere Clouds sorgen und übergreifende Visibilität vermitteln.

Inwiefern sehen Sie das «Zero Trust»-Modell als realisierbar für Unternehmen unterschiedlicher Grössenordnungen? Welche spezifischen Implementierungs-Herausforderungen haben Sie bei Ihren Kunden beobachtet?

Zero Trust ist naturgemäss etwas komplizierter, als einfach Netze zu koppeln. Es kommt darauf an, wo Zero Trust stattfindet und wie es stattfindet: nur für Zugriffe und Schnittstellen von aussen aufs Firmennetzwerk - dort ist Zero Trust unabdingbar - oder auch intern, was die Komplexität erhöht? Mit Segmentierung und geeigneten Verwaltungstools lässt sich auch dies weitgehend erreichen, sodass keine unnötigen Systemzugriffe mehr möglich sind. Teil dieser Tools sind Privileged-Access-Management-Lösungen (PAM), die zunehmend auch im Bereich OT (industrielle Anwendungen) zum Zug kommen.

Der Fachkräftemangels in der Cybersicherheit wird sich in den kommenden Jahren noch verschärfen. Welche innovativen Ansätze sehen Sie bei der Rekrutierung und Ausbildung von Talenten? Wie integrieren Sie KI-gestützte Automatisierung, um diesem Mangel entgegenzuwirken?

Ich weiss nicht, ob sich der Fachkräftemangel überhaupt noch verschärfen kann (lacht). Die zunehmende Komplexität der Systeme und das explosionsartig wachsende Volumen an Warnmeldungen und Problemen binden mehr Kräfte, als sie eigentlich sollten. Wir müssen also versuchen, effizienter zu werden. Ich glaube, dass KI zum Hilfsarbeiter der Security wird und gemeinsam mit dem Trend weg von Einzellösungen für jedes Problem hin zu umfassenden Plattformen helfen kann. Die Technik wird sich hier weiterentwickeln und die Security-Spezialisten entlasten.

> ***«Ich glaube, dass KI zum Hilfsarbeiter der Security wird und gemeinsam mit dem Trend weg von Einzellösungen für jedes Problem hin zu umfassenden Plattformen helfen kann.»***

Punkto Rekrutierung müsste das Informatikstudium attraktiver werden. Jungen Menschen müsste vermittelt werden, dass IT und Cybersecurity spannende Technologien sind und dass sie mit einer entsprechenden Ausbildung beste Chancen am Arbeitsmarkt haben. Die Verantwortung liegt dabei beim Bildungswesen, aber auch bei IT-Industrie bis hin zu uns als Distributor.

Welche technologischen Entwicklungen haben aus Ihrer Sicht das grösste Potenzial, das Thema Sicherheit in den kommenden Jahren nachhaltig zu prägen?

Das ist grundsätzlich nicht vorhersehbar. Im Moment beeinflusst KI die IT allgemein am meisten - es ist eine ganz andere Art, wie der Computer mit Daten umgeht im Vergleich zur traditionellen deterministischen Arbeitsweise. Das wird schwer abzuschätzende Auswirkungen haben. Was nach KI als grosses Thema kommt, kann heute noch niemand sagen.

Zum Schluss des Interviews haben Sie zwei Wünsche frei. Wie sehen die aus?

Ich wäre froh, wenn wir wieder zu einer Diskussionskultur zurückfinden könnten, statt alles via Social Media laut herauszuposaunen. Themen mit Fakten hinterlegen, fair diskutieren und sich auf Lösungen konzentrieren, statt nur schwarz-weiss zu denken.

Thomas Boll bei Linkedin