carmasec

security. done. right.

Interview mit Dr. André Schweizer

Gründer & Geschäftsführer von qbound

In unserer Interviewreihe stellen wir Ihnen regelmäßig junge Teams und deren Produkte und Leistungen vor.

Die drei Gründer des Startups qbound haben es sich zur Aufgabe gemacht, Organisationen den sicheren Zugang zu Cloud Diensten, Servern und IoT-Geräten zu ermöglichen. Dazu haben sie eine Plattform-Architektur entwickelt, die mittels der Blockchain Technologie einen Zero Trust Ansatz verfolgt.

Im Interview sprechen wir mit Dr. André Schweizer, Geschäftsführer von qbound.

1. Wie habt ihr euch als Gründerteam gefunden, habt ihr euch im Studium kennengelernt?

Dr. André Schweizer, CEO qbound

Wir als Gründerteam kennen uns nun bereits über mehrere Jahre hinweg, sowohl privat als auch im beruflichen Umfeld. Artur und ich haben bereits zusammen im Master studiert. Sven habe ich anschließend im Rahmen unserer Forschungs- und Doktorarbeiten bei Fraunhofer kennengelernt.

2. Wie seid Ihr auf den Namen qbound gekommen und was war eure Intention, ein eigenes Unternehmen im Security Bereich zu gründen?

Der Name qbound ist ein Kunstname, mit dem wir uns alle 100%ig identifizieren können. Es war uns wichtig, einen knackigen, sprechenden Namen für unsere Firma zu finden, der nach Möglichkeit auch noch relativ kurz ist. Wir denken, dass uns das gelungen ist.

Schon lange vor dem „finalen“ Gründungsvorhaben hatten wir uns darauf verständigt: Sollte sich eine Möglichkeit ergeben bzw. wir eine Chance für eine gemeinsame Gründungsinitiative sehen, werden wir diese beim Schopfe packen. Diese Situation ergab sich dann vor mittlerweile gut eineinhalb Jahren. Sven und ich waren auf der Zielgeraden unserer Promotion, Artur auf der Suche nach neuen Herausforderungen. Ein ebenso wichtiger Grund: Unternehmen sind auf der Suche nach einer zukunftssicheren Lösung im Bereich Identity und Access Management.

3. Welches sind die Grundvoraussetzungen, damit Access Management erfolgreich bei einem Unternehmen implementiert werden kann?

Accessmanagementlösungen an sich gibt es ja bereits einige Zeit. Das Besondere an unserem Produkt ist, dass es auf dem sogenannten Zero Trust Konzept basiert. Für unsere Accessmanagementlösung gilt der Grundsatz, immer erst zu authentifizieren, bevor Zugriff gewährt wird - egal, ob innerhalb des Unternehmensnetzwerks oder bei Zugriff von außerhalb. Damit dieses Konzept erfolgreich umgesetzt werden kann, braucht es zunächst insbesondere eines: den Willen zur Veränderung im Unternehmen, um es für das digitale Zeitalter zu wappnen. Es muss das Commitment der verantwortlichen Personen gegeben sein. Dann ist es meist kein Problem, die technischen Voraussetzungen wie ein Überblick über vorhandene Identitäten und Berechtigungen im Unternehmen herzustellen.

4. Die Digitalisierung zahlreicher Geschäftsfelder stellt viele Unternehmen vor große Probleme. Wie kann qbound diese Unternehmen bei den Herausforderungen der Digitalisierung unterstützen und Digitalisierungsrisiken minimieren?

Für die meisten Unternehmen bietet die Digitalisierung nicht nur eine Vielzahl an Chancen, sondern bringt auch große Herausforderungen mit sich. Das können beispielsweise die Bewahrung der Kontrolle und des Überblicks über hybride, also unterschiedliche IT-Infrastrukturen (On-Premise, Cloud, IoT) sein. Weiterhin müssen sich Unternehmen gegen Cyberkriminalität wappnen, indem sie ihre IT-Systeme adäquat absichern. Hier bietet unser Produkt eine ganz elementare Hilfe, da ein zukunftsfähiges Identity und Access Management die Grundlage für viele Prozesse im Unternehmen bildet. Wir geben eine Übersicht darüber, wer wann auf welche Systeme zugreifen darf und machen das Verwalten dieser Zugriffe spielend einfach. So können mit qbound temporäre Zugriffe leicht ermöglicht und wieder entzogen werden, die Sicherheit bei der Integration von IoT-Geräten verbessert werden oder eben auch Compliance-Anforderungen leichter überprüft werden.

5. Die Anzahl an IT-Sicherheitslösungen nimmt stetig zu. Welches konkrete Problem soll mit den Lösungen von qbound gelöst werden und wie unterscheiden sich diese von anderen Anbietern auf dem Markt? Bei welchen konkreten Anwendungsfällen soll eure Lösung idealerweise eingesetzt werden und wo liegen die Vorteile eures Ansatzes?

Wir sind derzeit der einzige deutsche Anbieter einer Zero Trust Identity und Access Management Lösung. Das Zero Trust Konzept weist enorme strukturelle Sicherheits- und Administrationsvorteile gegenüber bestehenden IT-Sicherheitslösungen auf.

Zur Verdeutlichung der Schwachstellen heutiger Herangehensweisen eignet sich eine Analogie aus einem sehr klassischen Bereich: Früher wurden Stadtmauern gebaut, um Städte gegenüber Eindringlingen zu sichern (abzuschotten). Um in eine Stadt zu gelangen existierten definierte Zugänge (Stadttore), an denen nur Berechtigten der Zugang gewährt wurde. In unserer Analogie stehen Städte für Organisationen und Mauern für traditionelle Firewalls, die eine strikte Trennung von internen und externen Netzwerken ermöglichen. Die Stadttore repräsentieren VPN-Verbindungen, die Berechtigten Zugang zur Stadt, also in das interne Netzwerk erlauben.

Schaffte es ein Betrüger bspw. durch eine falsche Identität, ein trojanisches Pferd oder einen Tunnel in die Stadt, so konnte er sich dort relativ frei bewegen und sein Unwesen in der gesamten Stadt treiben. Analog verhält es sich, wenn sich ein Angreifer Zugang in ein klassisch gesichertes Netzwerk verschafft: Er hat Zugriff auf große Teile des gesamten, internen Netzwerks und kann (potenziell) sämtliche Netzwerkkommunikation und IT-Systeme identifizieren, manipulieren und schädigen. Noch komplexer wird die Situation, wenn zur Integration externer Dienste und Smartphones/Notebooks eine Vielzahl von Schnittstellen eingerichtet werden müssen. Dadurch ähnelt die Stadtmauer zunehmend einem löchrigen Schweizerkäse.

Das qbound Gründer-Team v.l.n.r.: Dr. André Schweizer (CEO), Dr. Sven Radszuwill (CFO), Artur Rösch (CTO)

Wir von qbound entwickeln eine Lösung, die einzelne Applikationen individuell absichert. Diese erhöht die Sicherheit jedes einzelnen „Stadthauses“, anstatt eine große Stadtmauer zu bauen. Dadurch ermöglichen wir zum einen eine feingranulare Administration von Zugriffen. Zum anderen bleiben in dem Fall, in dem ein Angreifer es dennoch schafft sich Zugang zu einer Applikation zu verschaffen, alle anderen Applikationen vor ihm verborgen und geschützt. Dadurch verringern wir das IT-Sicherheitsrisiko enorm und erleichtern gleichzeitig die Administration von Applikationen und Unternehmensnetzwerken.-

6. Was sind eure Zielkunden bzw. wo seht ihr den höchsten Bedarf an einer Access Management Lösungen?

Es ist immer wieder erstaunlich, dass über die Hälfte der deutschen Unternehmen noch gar kein Identity und Access Management nutzen. Hier setzen wir an und wollen insbesondere dem deutschen Mittelstand helfen, direkt mit State-of-the-Art Lösungen zu arbeiten und nicht auf veraltete und unpassende Lösungen setzen zu müssen.

Gerade im Mittelstand, also bei Unternehmen zwischen 250 und 5000 Mitarbeitern, sind oft wenige IT-Mitarbeiter für die gesamte Unternehmens-IT verantwortlich und müssen mit enormen Komplexitäten umgehen. Genau diese Komplexitäten in der Nutzerverwaltung, dem Netzwerkmanagement und bei Remotezugriffen können wir deutlich verringern und dem IT-Personal damit einen signifikanten Teil ihrer Arbeit abnehmen. Gleichzeitig erhöhen wir das Sicherheitslevel im Unternehmen deutlich. Darüber hinaus planen wir ab Mitte kommenden Jahres das Angebot unserer Lösung als Software as a Service (SaaS) anzubieten. Hierdurch werden Nutzung und Integration unserer Lösung noch einfacher.

7. Häufig sind bereits Ansätze technisch und organisatorischer Maßnahmen im Bereich Access Management vorhanden. Wie lässt sich Access Management von qbound in bereits bestehende Infrastrukturen integrieren und nach welchem Preismodell werden eure Lösungen lizensiert?

Unternehmen, die bereits Access Management Ansätze für bestimmte Bereiche ihres Unternehmens implementiert haben (z.B. für On-Premise Applikationen) oder grundlegende Funktionen wie Multi-Faktor-Authentifizierung nutzen, haben bereits erste Schritte in die richtige Richtung getan. Aber auch hier können wir einen großen Mehrwert schaffen, indem wir unseren Kunden helfen, den nächsten wichtigen Schritt im Rahmen der Digitalisierung zu gehen.

Hierbei stehen insbesondere die nachfolgenden Eigenschaften unserer Lösung im Blickpunkt:

- **Einheitliche Sicht für alle Infrastrukturen:** Unsere Software ist Infrastruktur-agnostisch nutzbar. Sprich: Wir schaffen einen Überblick über alles Applikationen im Unternehmen (inklusive der genutzten Cloud-Applikationen und IoT Geräte). Dieser ganzheitliche Ansatz vereinfacht nicht nur die Administration enorm, sondern ermöglicht auch die vollständige Automatisierung beim Erkennen von Ungereimtheiten, wie kritischen Berechtigungskombinationen.
- **Authentifizierung bereits vor dem eigentlichen Verbindungsaufbau:** Mit unserer Lösung sind wir in der Lage, Applikationen und Geräte solange zu „verstecken“, bis ein Nutzer erfolgreich authentifiziert wurde. Dies bedeutet, dass dem Nutzer erst nach erfolgreicher Authentifizierung die Information, wo und wie die gewünschte Applikation erreicht werden kann, zur Verfügung steht. So werden ein unberechtigter Zugriff und das Angreifen einer Applikation quasi unmöglich. Das alles passiert automatisch und ist für den Endnutzer nicht wahrnehmbar.
- **Filterung von ein- und ausgehenden Daten:** Wir haben einen neuartigen Ansatz entwickelt, der es unseren Kunden ermöglicht, nicht nur die vollständige Kontrolle über die zugreifenden Nutzer und Geräte zu behalten, sondern zudem auch sicherstellt, dass keine sensible Daten aus System „abgesaugt“ werden und unberechtigterweise das Unternehmen verlassen.

8. Vertrauen ist in Zeiten digitaler Strukturen ein hohes Gut geworden. Welchen Vorteil bringt mir hier ein Zero Trust Ansatz?

Diese Entwicklung sehen wir auch in unserem alltäglichen Arbeiten. Bei all den zunehmenden Gefahren durch Cyberkriminalität ist dies auch absolut nachvollziehbar. Die Besonderheit und das Schöne an unserer Zero Trust Lösung ist, dass das System grundsätzlich niemandem traut und auch kein Vertrauen voraussetzt. Sprich, bei jeder Zugriffsanfrage – egal ob aus dem Firmennetz oder von extern – werden eine Reihe von Parametern wie das Nutzerprofil, der benutzte Computer und der Standort des Zugriffs überprüft. Basierend auf einem sicheren Algorithmus wird entschieden, ob es sich wirklich um einen berechtigten Nutzer handelt und ob Zugriff gewährt werden sollte.

9. Durch das Internet of Things kommunizieren unzählige Devices über das Internet miteinander. Wie kann qbound sicherstellen, dass nur Daten zwischen vertrauenswürdigen Geräten ausgetauscht werden und diese weder verändert noch mitgelesen werden können? Welche Vorteile bieten mir „over-the-air" Updates?

Der Schritt zum Internet of Things (IoT) wurde weitestgehend vollzogen. Wir stellen hierbei fest, dass in vielen Fällen „nicht smarte" Geräte einfach ans Internet angebunden wurden, ohne sich über Sicherheitskonzepte Gedanken zu machen. Dies ist nicht nur bei vermeintlich banalen Dingen wie TVs und Kühlschränken, sondern unter anderem auch im Bereich der kritischen Infrastrukturen wie bei Windparks, Solaranlagen und Kraftwerken, passiert. In all diesen Bereichen lassen sich unzureichende Cybersecurity-Konzepte finden und die Liste erfolgreicher „Hacks" durch Kriminelle ist lang. Um dieses Problem zu lösen haben wir unsere Zero Trust Lösung so entwickelt, dass sie auch im IoT genutzt werden kann. Wir haben sicherstellt, dass nur authentifizierte Geräte Daten austauschen können. Zudem separiert unsere Lösung einzelne (z.B. durch Hardwareeingriffe) kompromittierte Geräte sofort, sodass keine anderen Geräte infiziert werden können.

Die qbound Gründer als Teil des Mentorship Programms von Startup Inkubator Cube5 (© Cube 5/Ruhr-Universität Bochum)

Unsere Welt ist eigentlich heute schon ohne „over-the-air" Updates gar nicht mehr denkbar. Ein Beispiel sind Smartphones, die sich ständig auf diese Weise aktualisieren– „over-the-air" Updates machen den gesamten Prozess schlanker und schneller. Wir stellen in diesem Prozess sicher, dass nur authentifizierte und berechtigte Parteien Update ausführen können, die Datenübertragung sicher abläuft und keine Manipulation am Update erfolgt. Zudem ist jederzeit nachvollziehbar, wer welche Aktion ausgeführt hat.