carmasec

security. done. right.

Interview mit Felix Brombacher

Co-Gründer von Crashtest Security

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

Crashtest Security ist ein Münchner Startup für IT-Sicherheit, das sich auf Sicherheitsüberprüfungen von modernen Webanwendungen spezialisiert hat. Die automatisierten Tools zur Schwachstellenanalyse basieren auf einer intelligenten Logik zur Erkennung der Sicherheitslücken und tragen so zu einem besseren Schutz gegen Cyberangriffe bei.

Im Interview sprechen wir mit Felix Brombacher, Co-Gründer von Crashtest Security.

1. Euer Unternehmen wurde im Jahr 2017 von vier Partnern gegründet. Wie habt ihr euch kennengelernt und wie verteilt ihr die Aufgaben im Team?

Felix Brombacher, Co-Founder Crashtest Security

Unser Gründerteam besteht aus Janosch Maier, Daniel Schosser, René Milzarek und mir. Janosch und Daniel kenne ich schon seit meiner Kindheit. Wir haben uns bei ehrenamtlichen Tätigkeiten in unserem Heimatdort Gilching getroffen. Janosch und Daniel haben René dann während ihres Informatik-Studium in München kennengelernt.

Als Team organisieren wir uns stark themenfokussiert. Aufgaben verteilen wir nach Fachgebieten. Janosch verantwortet als Product Owner den Customer Success. Daniel entwickelt das Backend und ist Lead Developer für die Scanner Software. René kümmert sich um das Frontend und die Software Architektur. Ich verantworte kaufmännische Themen wie Vertrieb, Marketing und Finanzen.

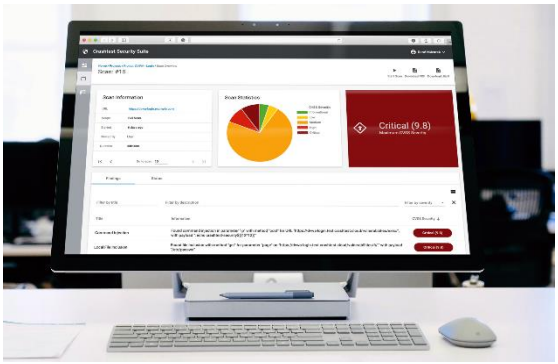
2. Was war bei euch der Auslöser zur Unternehmensgründung und was motiviert euch am Unternehmersein besonders?

Es gibt tatsächlich einen initialen Auslöser für die Gründung unseres Unternehmens: Janosch, Daniel und René nahmen im Rahmen ihres Studiums an einem Seminar mit dem Titel „Secure Coding“ teil. Alle Teilnehmer entwickelten eine Banking-App, die im Nachgang gehackt wurde. Zur Sicherung ihrer App haben Janosch, René und Daniel den OWASP Testing Guide genutzt. Um das Security Testing ihrer App zu vereinfachen, suchten sie einen einfach zu bedienenden Sicherheitsscanner. Diesen gab es jedoch nirgends in Netzt zu finden, da zu diesem Zeitpunkt nur sehr teure Großkunden-Lösungen auf dem Markt erhältlich waren. Also setzten sie sich das Ziel, einen solchen Scanner zu bauen. Ich bin etwas später mit Start des „Exist Gründerstipendiums“ zum Team hinzugestoßen.

3. Das Risiko, von ausnutzbaren Schwachstellen und Sicherheitslücken betroffen zu sein, steigt ständig. Umso wichtiger ist eine umfassende Gesamtstrategie, um wirksame Maßnahmen zur Risikominderung zu implementieren. Mit eurem Lösungsansatz könnt ihr sowohl IT-Fachkräften wie Softwareentwicklern und -testern als auch Führungskräften wie dem CISO oder IT-Leiter die Arbeit erleichtern. An welcher Stelle werden eure Vorteilsversprechen am dankbarsten aufgenommen?

Leitende Personen nehmen die Vorteile unseres Scanner Einsatzes am ehesten an, da sie meist die Verantwortung für den Schutz wichtiger Daten (z.B. Firmendaten oder personenbezogene Daten) tragen. Der Einsatz unserer Software lässt sie „ruhiger schlafen".
Aber auch Entwickler setzen unsere Lösung gerne ein, da es ihnen den Arbeitsalltag erleichtert und händisch aufwändige Sicherheitsaufgaben automatisiert.

4. Eure cloud-basierte Lösung lief anfänglich in der AWS (Amazon Web Services) und ihr seid dann zur GCP (Google Cloud Platform) migriert. Warum habt ihr diesen Schritt gemacht und wie waren eure Erfahrungen beim Wechsel des Cloud Service Providers? Wie aufwendig war das für euch als „Cloud Natives"?



Ergebnisse eines Scans mit der Crashtest Security Suite

Der primäre Grund für den Umzug war das Start-Up Programm von Google. Damit können wir unsere Infrastruktur für ein Jahr kostenlos betreiben. Zudem nutzen wir Google-native Technologien wie beispielsweise „Kubernetes", die auf der GCP deutlich stabiler laufen. Wir hatten damals unerklärliche Ausfälle bei AWS, die nach der Migration nicht mehr auftreten.

Der Umzug selbst war recht aufwendig und hat uns ungefähr drei Mann-Monate gekostet. Allerdings haben wir auch sehr sorgfältig geplant, damit trotz limitierter Ressourcen das Tagesgeschäft uneingeschränkt weiter bedient werden konnte.

5. Mit eurer Lösung adressiert ihr den wachsenden Bedarf an automatisierten Softwaretests überwiegend in agilen Entwicklungslandschaften. Es gibt auf dem Markt eine ganze Reihe an SAST-/DAST-Lösungen, die überwiegend aus dem amerikanischen Raum stammen. An welchen Stellen seid ihr besser und was sind eure Alleinstellungsmerkmale?

Wir sind der einzige Anbieter, der auf JavaScript basierende Frontends komplett automatisiert crawlen und testen kann. Andere Anbieter können dies gar nicht oder benötigen z.B. zusätzliche Klick-Modelle, welche mühsam aufgezeichnet werden müssen. Außerdem lässt sich unsere Software besonders gut in den agilen Entwicklungszyklus integrieren und ermöglicht so die Umsetzung einer agilen Security Strategie.

Hinsichtlich der Anforderung an DSGVO-Konformität können wir noch einen entscheidenden Vorteil verbuchen: Wir sind der einzige Anbieter, der aus Deutschland agiert. Unsere Produkte sind komplett „made & hosted in Germany“ und dies wird von Entscheidern oft gesucht.

6. Mit der agilen Softwareentwicklung und dem Zusammenwachsen von Entwicklung und Betrieb (DevOps) kommt häufig das Thema Sicherheit noch immer zu kurz. Müsst ihr bei euren Kunden in der Richtung noch Überzeugungsarbeit leisten, warum es sinnvoll ist, ein SAST-/DAST-Tool einzusetzen? Oder ist dieser Bedarf bei euren Kunden schon erkannt worden?

Das Crashtest Security Team

Nur wenige Kunden sehen den vollen Bedarf und die Vorteile des Scanners für die automatisierte Überprüfung eines jeden Software Releases. Allerdings werden die Unternehmen immer stärker durch den Markt sensibilisiert.
Viele Firmen fühlen sich in der Cloud wohl und vertrauen dieser mehr und mehr. Dies führt in der Konsequenz dazu, dass sie sich auch mehr mit dem Thema Security beschäftigen müssen. Regulatorische Vorgaben wie z.B. die DSGVO verstärken diesen Trend noch weiter.

7. Durch die Fokussierung auf DevSecOps und die automatisierte Form von Penetrationstests müssen eure Kunden auch ein „agiles Mindset“ oder zumindest eine Affinität zur Nutzung von Cloud-Diensten mitbringen. Wie schätzt ihr diesbezüglich den Reifegrad von europäischen Unternehmen im Vergleich zu internationalen oder amerikanischen Unternehmen ein? Und gibt es hier wesentliche Unterschiede zwischen großen und kleinen bzw. etablierten und jungen Unternehmen?

Im europäischen Vergleich befinden sich deutsche Unternehmen meiner Meinung nach hinsichtlich eines agilen Mindsets im unteren Mittelfeld. Ähnlich verhält es sich im Vergleich europäischer zu amerikanischen Unternehmen. Deshalb sehen wir auch viel Wettbewerb vor allem aus dem amerikanischen Raum.

Auf der anderen Seite ist aktuell sehr viel Bewegung im europäischen Markt. Viele Unternehmen befinden sich in der digitalen Transformation und migrieren Daten und Infrastruktur zu Cloud-Diensten. Dies bedeutet, dass sich in den kommenden drei Jahren in der EU einiges bewegen wird. Junge Unternehmen sind hier auch deutlich weiter als der Mittelstand. Große Konzerne haben zwar häufig sehr gute Strategien, allerdings auch große Altlasten und oftmals keine passende Softwarelösungen, welche nach der Umstellung weiter genutzt werden.

8. Euer Produkt ist sowohl in einer Cloud basierten SaaS-Lösung als auch als On-Premise-Appliance zu beziehen. Wie verteilt sich hierbei die Nachfrage?

Wir bieten neben der Cloud-Version eine hybride On-Premise-Lösung an. Da diese deutlich teurer ist, entscheiden sich die meisten Unternehmen für die Cloud-Variante und weichen damit häufig von ihrem „bei uns ist nur On-Premise möglich“-Dogma ab.

9. Welche wesentlichen Meilensteine und Funktionalitäten können wir von euch noch erwarten? Woran arbeitet ihr derzeit?

Aktuell stehen Funktionen wie ein verbessertes „False Positive Marking“ sowie ein „Customizable Reporting“ auf der Roadmap. Außerdem wollen wir den Prozess zur Tool-Einführung weiter verbessern, damit die Nutzer noch schneller ihre Anwendungen absichern können. Langfrist ist der Einsatz von smarten Algorithmen geplant, um komplexe Angriffsszenarien zu simulieren.

10. Wie schätzt ihr die weitere Entwicklung im IT-Markt ein: werden wir alle zukünftig „Cloud Natives“ in Multi-Cloud-Umgebungen? Und welche Auswirkungen hat dies hinsichtlich wirksamer Maßnahmen zur Abwehr von Cyberangriffen?

Der Trend geht ganz klar hin zu Cloud-Services. Dem werden sich die meisten Unternehmen nicht entziehen können. Damit steigt natürlich die Gefahr von Cyberattacken. Neben einer agilen Entwicklung benötigen Unternehmen auch eine agile Security-Strategie, da Cybersicherheit immer ein Wettrennen gegen die Angreifer sein wird.

Wir danken für das Gespräch!

Weitere Informationen zum Startup Crashtest Security finden Sie auf ihrer Website