# « Anbieter müssen strenge Sicherheitsprotokolle einhalten »

Nevena Shamoska ist Mitgründerin und Chief Technical Officer von PXL Vision und kümmert sich um die technische Weiterentwicklung der verschiedenen Lösungen. Im Interview erklärt sie, worauf IT-Dienstleister achten sollten und welche Eigenschaften besonders wichtig sind. Interview: René Jaun

**Was beinhaltet Ihre tägliche Arbeit und wo kommen Sie mit IT-Dienstleistern in Berührung?**
Nevena Shamoska: In meiner täglichen Arbeit konzentriere ich mich auf die Entwicklung von SaaS-Technologien und -Produkten, die eine Remote-Identitätsprüfung und einen End-to-End-QES-Service ermöglichen. Dies beinhaltet die Verwaltung und Verbesserung von maschinellen Lernmodellen, die Gewährleistung sicherer und reibungsloser Prozesse der Identitätsprüfung und die Aktualisierung unserer Software mit den neuesten Sicherheits- und Compliance-Standards. Ich arbeite hauptsächlich mit IT-Dienstleistern zusammen, wenn es um Cloud-Infrastruktur, Sicherheitslösungen und die Integration externer Dienste zur Verbesserung der Performance und Datenverarbeitung geht. Diese Zusammenarbeit ist entscheidend, um die hohe Leistung, Skalierbarkeit und Zuverlässigkeit unseres Produkts aufrechtzuerhalten und gleichzeitig kontinuierliche Aktualisierungen und Verbesserungen durch unsere internen und externen technischen Teams zu unterstützen.

« Mangelnde Transparenz und schlechte Kommunikation können das Vertrauen untergraben und eine effektive Zusammenarbeit behindern. »

Nevena Shamoska, Mitgründerin, Chief Technology Officer, PXL Vision

**Welches sind die drei wichtigsten Eigenschaften, die Ihre IT-Dienstleister mitbringen müssen?**
Erstens ist die ständige Verfügbarkeit von entscheidender Bedeutung, da es sich bei unserem Produkt um eine SaaS-basierte Lösung zur Fernverifizierung von Identitäten handelt. Die Dienstleister müssen eine hohe Verfügbarkeit, eine konstante Leistung und eine schnelle Reaktion auf Probleme gewährleisten, um sicherzustellen, dass unsere Plattform für die Nutzer jederzeit zugänglich ist. Zweitens müssen die Anbieter aufgrund der Sensibilität der Identitätsdaten strenge Sicherheitsprotokolle einhalten, einen robusten Schutz vor potenziellen Verstössen bieten und relevante Vorschriften wie ZertES, eIDAS oder GDPR einhalten. Dies trägt zum Schutz der Nutzerdaten bei und stärkt das Vertrauen in unsere Lösung. Drittens ist es angesichts der Weiterentwicklung unserer Plattform und der schwankenden Nutzernachfrage wichtig, dass unsere IT-Dienstleister die Skalierbarkeit und ein flexibles Ressourcenmanagement unterstützen. Sie sollten eine schnelle Skalierung ermöglichen, um steigende Arbeitslasten zu bewältigen, und gleichzeitig eine nahtlose Integration in unsere Systeme ermöglichen, wenn unsere Produkt- und Geschäftsanforderungen wachsen.

**Was sollten (potenzielle) IT-Partner tunlichst vermeiden?**
Ich würde sagen, dass mangelnde Transparenz und schlechte Kommunikation das Vertrauen untergraben und eine effektive Zusammenarbeit behindern können. Für uns ist es wichtig, eine offene Kommunikation zu pflegen, insbesondere in Bezug auf Servicefragen, Updates oder Änderungen. Unzuverlässige Dienste, häufige Ausfallzeiten oder eine instabile Performance können die Verfügbarkeit und das Nutzererlebnis unseres SaaS-Produkts erheblich beeinträchtigen. Jede Störung kann zu Geschäftseinbussen, Vertrauensverlust bei Kunden und Rufschädigung führen. Da wir mit sensiblen Identitätsdaten arbeiten, ist es für uns inakzeptabel, Sicherheitsmassnahmen und Compliance-Anforderungen keine Priorität einzuräumen.

**Welche Bereiche Ihrer Unternehmens-IT haben Sie ausgelagert?**
Wir lagern bestimmte Aspekte der Infrastruktur aus, zum Beispiel die Einrichtung und Wartung der Cloud, um einen zuverlässigen Betrieb und ein effizientes Ressourcenmanagement zu gewährleisten. Ein Teil unserer Entwicklungsarbeit für bestimmte Funktionen und Produktverbesserungen wird von externen Softwareingenieuren übernommen.

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