carmasec

security. done. right.

Interview mit Markus Hertlein

Geschäftsführer von XignSys

Im Rahmen von Mentorships unterstützen wir junge Startups auf ihrem Weg von der innovativen Idee zum marktreifen Produkt. In einer Interviewreihe möchten wir Ihnen drei Unternehmen, deren Gründer und kreative Ideen uns überzeugt haben, vorstellen.

Das erste Unternehmen, welches Einblicke in seine Arbeit gibt, ist die XignSys GmbH mit Sitz in Gelsenkirchen. Die innovativen Gründer bieten mit der von ihnen entwickelten Technologie XignQR eine Lösung zur zentralen Identifikation von Benutzern mittels QR-Codes. Das Startup entwickelt damit die nächste Generation einer anwenderfreundlichen und starken Authentifizierung für Transkationen, eSignaturen und digitale Identitäten.

1. Ihr seid als Startup angetreten, um das verhasste Passwort abzulösen. Was unterscheidet euch von allen anderen Wettbewerbern, die ebenfalls im Bereich Authentifizierung aktiv sind?

Markus Hertlein, CEO XignSys

Aus unserer Sicht sind wir direkt den weiteren Weg gegangen und haben unsere wissenschaftlichen Erkenntnisse aus 10 Jahre IT-Security-Forschung in ein Produkt gegossen. Ziel war es mit XignQR eine Technologie und Produkt auf den Markt zu bringen, die den höchsten Ansprüchen an Sicherheit und an Benutzerfreundlichkeit genügt.

Neben den höchsten Schlüssel- und Krypto-Algorithmen, wie ECC571, AES256, SHA-3 mit 512 Bit, war es uns wichtig eine Authentifizierungslösung anzubieten, die in wirklich jedem Anwendungsfall genutzt werden kann, um die Sicherheit und Benutzerfreundlichkeit zu erhöhen.

Durch die einzigartige Beyond-Token Technologie, die mit Auslösern wie dem QR Code, aber auch NFC, Bluetooth und Co. arbeiten, eben allem was mit dem Smartphone interagieren kann, ermöglichen wir eine einfache und sichere Authentifizierung für Webseiten und Portale, am PC, Laptop oder Smart Device, aber auch für e-Government-Anwendungen, IoT, Smart City, e-Mobility und weiteren.

2. Könnt ihr kurz skizzieren, wie eure Lösung technisch funktioniert und welche Verfahren zum Einsatz kommen?

Aus technischer Betrachtung wird bei der Authentifizierung ein kryptographisches Frage-Antwort-Spiel durchgeführt, ein sogenanntes Challenge-Response-Verfahren auf der Basis eines asymmetrischen kryptografischen Schlüsselpaares. Als Grundlage dient eine Public-Key-Infrastruktur, die unfälschbare Zertifikate für die kryptografischen Schlüssel und den Besitzer ausstellt. Letztendlich wird eine Smartphone App einmalig bei der Inbetriebnahme mit mehreren

kryptografischen Schlüsseln und korrespondieren digitalen Zertifikaten versehen. Damit erhält das Smartphone eine digitale Identität, jedes Authentifizierungsmerkmal eine digitale Identität und der Nutzer selbst. Bei der Integration in einen Dienst geschieht dasselbe für den Dienst und Server.

Um den Komfort weiter zu steigen, bietet XignQR die Möglichkeit Single-Sign-On (SSO) in der Kombination mit kontextbasierter und Step-Up Authentifizierung zu nutzen, so wie den vergesslichen Nutzer sich remote per App an seinem System auch wieder auszuloggen, ähnlich wie man es von den großen amerikanischen Plattformen wie Facebook oder WhatsApp kennt. Zu erwähnen ist noch, dass alle Daten digital unterschrieben werden und doppelt verschlüsselt innerhalb einer Session übertragen werden. So werden die gesamte Authentifizierung und Kommunikation vor Fälschung und Einsicht geschützt.

3. Könnt ihr kurz einen Überblick geben, wer aus eurer Sicht der ideale Zielkunde für eure Lösung ist und in welchem Kundenumfeld ihr bereits aktiv seid?

Das XignSys -Team (v.l.n.r.): Alexander Stöhr, Markus Hertlein und Pascal Manaras | https://etailment.de

Der perfekte Kunde bietet eine breite Nutzerbasis. Dabei spielt es keine Rolle ob es sich um interne Anwendungen oder externe handelt. Gerne kann es sich dabei auch um Endkundenanwendungen handeln. Sehr gute Erfahrungen haben wir aktuell im Bereich Automotive gemacht. Aufgrund der aktuellen Lage mit der PSD2 sind aber auch Banken und Zahlungsdienstleister höchst interessante Kunden. Aufgrund der Möglichkeit der Nutzung als On-Premise und SaaS bietet sich XignQR aber auch für mittlere und kleine Unternehmen an.

4. Wie aufwendig ist die Implementierung eurer Lösung für den Kunden? Und gibt es Ansatzpunkte bestehende unzufriedenstellend funktionierende Systeme durch eure Lösung abzulösen?

Wie zuvor kurz erwähnt kann XignQR häufig als „Plug & Play“ Lösung integriert werden. Sollte es aber aufgrund einer alten Infrastruktur Implementierungsarbeiten nötig sein, ist auch hier der Aufwand meist überschaubar, da wir SDKs für die meisten Anwendungen mitbringen. Für spezielle Anwendungen ist häufig auch die Variante eines Plug-Ins interessant. Somit sind wir breit aufgestellt, um den Integrationsaufwand möglichst gering zu halten. Neben dem Passwort steht häufig die Ablösung von Einmal-Passwort-Token (OTP) oder Chipkarten auf der Agenda. Es soll häufig die komfortable und dennoch sichere mobile Nutzung gewährleistet werden. Eine beliebte Anwendung ist hier der mobile Arbeitsplatz.

5. Wo positioniert sich eure Lösung wirtschaftlich im Vergleich zu anderen Lösungen in diesem Bereich? Was kostet einen Kunden die Abkehr vom klassischen Passwort?

Wir bieten drei Geschäftsmodelle, um auch hier flexibel auf Kundenbedürfnisse eingehen zu können. Je nachdem, ob es sich um die On-Premise- oder SaaS-Variante handelt, gibt es einmal die Möglichkeit eine Appliance oder Virtual-Appliance mit passender Software zu kaufen oder einfach und sehr komfortabel als Subscription auf Nutzerbasis abzurechnen.

Für transaktionsbezogene Anwendungsfälle, beispielsweise im B2C Bereich, kann auch ein Modell gewählt werden, welches auf Transaktionsgebühren basiert. Beim Subskriptionsmodell reicht die Spanne von 6 € pro Nutzer bis 0,12 € pro Nutzer pro Monat – gestaffelt nach Anzahl der Nutzer. Damit liegen wir deutlich unter den Preisen für hardware-basierte Systeme und auch im Vergleich zum Passwort sind wir recht günstig, wenn man betrachtet, dass die produktive Arbeitszeit maximiert wird und Ausfälle minimiert werden. Zudem entfallen teure und umständliche Kennwortrücksetzungen, ganz zu schweigen von Kosten, die einem Unternehmen durch erfolgreiche Angriffe über das schwache Passwortverfahren entstehen.

Sollte ein Unternehmen oder ein Zahlungsdienstleister einen schleichenden Übergang vom Passwort vornehmen oder auf das Passwort nicht verzichten wollen, kann XignQR auch als zweiter oder weiterer Faktor genutzt werden, dann auch ganz komfortabel per Authentifizierung via Push-Nachricht.