InnoSecBW

CYBERSECURITY-BOOSTER-BERICHT
MissionBuddies GmbH

Ein Projekt des

FZI

FZI Forschungszentrum Informatik
Haid-und-Neu-Str. 10–14
76131 Karlsruhe

Gefördert durch das

Baden-Württemberg
MINISTERIUM FÜR WIRTSCHAFT, ARBEIT UND TOURISMUS

Die MissionBuddies GmbH ist ein innovatives Unternehmen mit Sitz in Konstanz, das Softwarelösungen für verschiedene Rettungskräfte bereitstellt.

PROBLEMSTELLUNG

Die MissionBuddies GmbH entwickelt eine Anwendung namens FWApp, mit deren Hilfe Feuerwehren, Rettungshundestaffel und Drohnenstaffeln effektiv ihre Einsätze verwalten, dokumentieren und leiten können. Bei den erfassten Daten handelt es sich um personenbezogene und sehr sensitiven Daten, die außer den jeweiligen Leitstellen und Mitarbeitenden niemandem bekannt werden dürfen. So soll auch die MissionBuddies GmbH keinen Zugriff auf die Daten erhalten können.

Gleichzeitig müssen die Daten jedoch auch stets verfügbar sein, da bei einem Datenverlust potenziell Gefahr für Leib und Leben besteht.

Die MissionBuddies GmbH hat sich daher entschieden, die Daten zentral bei sich zu speichern, jedoch in verschlüsselter Form. Kenntnis des Schlüssels haben nur die jeweiligen Kunden, die die Entschlüsselung lokal durchführen. Damit können nur sie auf die Daten zugreifen, müssen sich jedoch nicht für die Speicherung der Daten verantworten, was die Wahrscheinlichkeit eines Datenverlusts aufgrund von Fehlern bei der Administration der Infrastruktur verringert.

Eine wesentliche Herausforderung bestand in der sicheren Synchronisation der Schlüssel auf den heterogenen Endgeräten der Kunden, welche bei manchen Kunden über verschiedene Standorte verteilt genutzt wurden.

Bei einer manuellen Eingabe der Passwörter, aus deren die Schlüssel abgeleitet werden, besteht das Risiko, dass aus Bequemlichkeit kurze, unsichere Passwörter eingesetzt werden. Bei langen Passwörtern hingegen, ergibt sich ein hoher Aufwand, um diese auf allen anderen Geräten einzugeben.

Stand der Technik und Vorgehen

In mehrere Workshops wurden gemeinsam mit der MissionBuddies GmbH die Herausforderungen und Bedrohungen für die Anwendung identifiziert. Besonderes Augenmerk wurde dabei auch auf Angreifermodelle gelegt, da die eingesetzten Geräte sowohl in den Einsatzfahrzeugen als auch vor Ort verwendet werden, sodass neben Online-Angreifern auch verschiedene physische Angreifer realistisch sind.

Mit den Informationen aus den Workshops haben die Mitarbeiter des FZI Forschungszentrum Informatik konkrete Angreifer modelliert und sich überlegt, wie Schutzmaßnahmen gegen diese Angreifer aussehen könnten. Die Maßnahmen wurden dann auf Praktikabilität und Akzeptanz bei den teilweise nicht IT-affinen Endanwendern überprüft und verworfen, falls diese von den Anwendern vermutlich nicht angenommen werden würden. Ebenso wurde versucht Lösungen, zu finden, welche keinen allzu großen Entwicklungsaufwand für die Entwickler der MissionBuddies GmbH bedeuten.

Auf dieser Grundlage wurde für den lokalen Schlüsselaustausch ein Verfahren auf Basis von einem Anzeigen und Ablesen von QR-Codes zwischen den Geräten gewählt, da dieses allen Anforderungen entsprochen hat.

Beim Schlüsselaustausch zwischen Geräten in unterschiedlichen Wachen oder Niederlassungen entstand ein Protokoll, welchem ein Diffie-Hellman-Schlüsselaustausch zugrunde liegt und welches die bestehende Infrastruktur der MissionBuddies GmbH nutzt, um die Kommunikation zwischen den Geräten herzustellen.

Zuletzt wurde ein Verfahren entworfen, um die verschlüsselten Daten im Falle eines Bekanntwerdens des Schlüssels zeitnah neu zu verschlüsseln, jedoch durchgehend auf allen Geräten verfügbar zu halten.

Erkenntnisse und Nutzen

Das FZI Forschungszentrum Informatik konnte im Verlauf des Cybersecurity-Boosters verschiedene Möglichkeiten erarbeiten, um die Problemstellung zu lösen. So wurden verschiedene Lösungen erarbeitet, welche das Problem mit zusätzlichem Aufwand auch vor mächtigeren Angreifern oder unter erschwerten Bedingungen lösen konnten.

Darüber hinaus haben die an dem Cybersecurity-Booster beteiligten Mitarbeiter des FZI Forschungszentrum Informatik das Unternehmen auf Bedrohungen durch Quantencomputer bei diesen und ähnlichen Lösungen hingewiesen und postquantensichere Alternativen vorgeschlagen. Diese Erkenntnisse und Hinweise gelten gleichermaßen auch für andere Entwicklerunternehmen, welche selbst Softwarebibliotheken für Kryptographie einsetzen.

Das FZI Forschungszentrum Informatik hat in Zusammenarbeit mit der MissionBuddies GmbH den sicheren Schlüsselaustausch zwischen heterogenen Systemen untersucht. Die gewonnenen Erkenntnisse können auch anderen Unternehmen dabei helfen, sensitive Daten zu verschlüsseln und zu speichern, um diese verfügbar aber sicher aufzubewahren und bereitzustellen.