Cybersicherheit und Datenschutz als Schlüsselelemente für höchste Qualität der MOBOTIX Videosysteme

03. April 2023

Langmeil, März 2023 – Die USA machte mit dem *National Defense Authorization Act (NDAA) den Anfang. Der NDAA listet zum Schutz vor chinesischer Spionage bestimmte Bauteile und Firmen auf, die für* Telekommunikationsausrüstungen (einschließlich Sicherheitsprodukte) oder Dienstleistungen nicht verwendet werden dürfen, um die Endprodukte an US-Bundesbehörden, ihren Auftragnehmern und Zuschuss- oder Darlehensempfängern und mit denen in Verbindung stehenden Einrichtungen zu verkaufen. Mit Großbritannien und Australien folgten weitere Länder diesem Beispiel, und auch die EU hat Ende letzten Jahres den Cyber Resilience Act (CRA) auf den Weg gebracht. Diese Unternehmen und Bauteile chinesischer Herkunft, die im NDAA aufgelistet sind, stehen im Verdacht, für die chinesische Regierung zur Ausspähung und Spionage eingesetzt werden zu können.

Die MOBOTIX AG bestätigt, dass alle MOBOTIX Videosysteme den Anforderungen des NDAA entsprechen und zu 100 Prozent NDAA-konform sind. MOBOTIX verwendet keine SoC (System on Chip) oder andere Komponenten, die Software von chinesischen Unternehmen verarbeiten können. Darüber hinaus sind MOBOTIX-Produkte, die von OEM-Partnern (Original Equipment Manufacturers) bezogen werden, ebenfalls 100% NDAA-konform. MOBOTIX hat in einem definierten 3-stufigen Selbstzertifizierungsprozess eindeutig nachgewiesen, dass seine Videoüberwachungskameras keine chinesischen Komponenten enthalten.

Die hohen Qualitäts-Standards werden auch vom renommierten australischen “Security Electronics & Networks Magazine (sen.news)” bestätigt, das sich wie folgt äußert: "*Nach Meinung von SEN ist die cybersicherste IP-Überwachungskamera Mobotix, … mit ihrer enormen operativen Flexibilität und ihren tadellosen Cybersicherheitsnachweisen.*"

Cybersicherheit und Datenschutz als zentrale Qualitätsmerkmale

Cybersicherheit ist fester Bestandteil der MOBOTIX DNA. Die MOBOTIX Videosysteme werden regelmäßigen Penetrationstests unterzogen, beispielsweise vom französischen Centre national de prévention et de protection (CNPP) und der SySS GmbH, dem führenden Institut für Penetrationstests in Deutschland. Alle MOBOTIX Produkte und Lösungen sind in die umfassende Cybersicherheits-Strategie eingebunden, deren Gesamtmaßnahmen im MOBOTIX Cactus Concept gebündelt sind https://www.mobotix.com/es/cactus-concept-cyber-security.

„Wir begrüßen die wachsende Sensibilität insbesondere von Regierungen sehr und auch Unternehmen haben die Gefahr der Wirtschaftsspionage längst erkannt.“, so Christian Cabirol, CTO der MOBOTIX AG. „Bereits seit vielen Jahren verwenden wir für unsere Hardware und Bildgenerierungsketten nur leistungsstarke industrielle FPGAs (Field Programmable Gate Arrays) und bieten damit einen zuverlässigen Schutz für den Anwender.“ Ein FPGA dient der kontinuierlichen Verarbeitung digitaler Signale wie Audio- und Videosignale, neuronaler Netzwerke und Deep Learning Algorithmen sowie Künstlicher Intelligenz und macht ein System weitaus unangreifbar für Hackerangriffe und Spionagesoftware. „Auf diesen Prozessoren kommt die proprietäre MOBOTIX Software ‚Made in Germany‘ zum Einsatz - und wir behalten so die volle Kontrolle darüber, was das gesamte System leistet und kann“, erläutert Cabirol.

Ebenso sorgt die dezentrale Architektur der MOBOTIX Videosysteme für beste Sicherheit, da alle Bildverarbeitungs-Prozesse, wie beispielsweise die Verpixelung von Personen, direkt auf der Kamera passieren und keine Übermittlung von unverpixelten Daten erfolgt. Überhaupt stehen datenschutz- und DSGVO-konforme Anwendungen im Fokus von MOBOTIX. So können Apps der MOBOTIX 7 Plattform Bilder sogar dynamisch verpixeln, indem sie Menschen erkennen und automatisch anonymisieren. Das kann bei der Überwachung sensibler Bereiche, von öffentlichen Plätzen oder Schulen wichtig sein. Auch Thermalanwendungen bieten beste Möglichkeiten für den DSGVO-konformen Perimeter- und Objektschutz, da Menschen im Thermalbild zwar zu sehen, aber nicht zu identifizieren sind. Die dezentrale Architektur erfordert zudem keinen dauerhaften Stream zu einem Server oder einer Zentrale, da Bilddaten nur bei einem Event übermittelt werden. Und dieser Dialog erfolgt stets verschlüsselt.