Videoüberwachung trifft auf Datenschutz

Die Leistungsfähigkeit von Überwachungskameras wächst mit jeder Modellgeneration und wo manche Fahndungsfotos älterer Systeme immer noch wie Bilder aus der frühesten Filmgeschichte anmuten, erkennen moderne Kameramodelle Gesichter, können Alter und Geschlecht einschätzen, Autokennzeichen lesen, erfassen Besucherzahlen auf Veranstaltungen und erstellen Bewegungsprofile der Kunden eines Supermarktes oder der Besucher von Museen.

Immer wieder werden Rufe nach mehr Videoüberwachung laut, wie jüngst wieder durch Innenminister Horst Seehofer, der eine stärkere Überwachung der Bahnhöfe fordert und für den Ausbau der Kamerasysteme bis 2023 ein Investitionspaket von 70 Millionen Euro in Aussicht stellt. Neben der Aufklärung soll die Videoüberwachung hier eher der Abschreckung dienen, mit der Vorfälle eher vermieden werden sollen, als sie im Nachhinein aufklären zu müssen. Zur Prävention wird hier unter anderem auch die automatische Gesichtserkennung gezählt, die zentral mit Daten gefüttert wird und frühzeitig unerwünschte Besucher erkennen soll.

Diskussionen über das Für und Wider einer Videoüberwachung werden in aller Regel sehr kontrovers geführt, gleicht es doch einem Spagat die Lager zwischen Sicherheit und Datenschutz zu vereinen. Tatsächlich wird das Thema Datenschutz mit immer moderneren Lösungen immer leichter, denn mit vielen Features in der Firmaware der Kameras und der dahintergelagerten Software, können viele Kritikpunkte ausgeräumt werden. So lassen sich nicht zu überwachende Bereiche schwärzen, Gesichter verpixeln oder eben auch Kameras und Software so eingestellt werden, dass die Speicherung der Aufgenommenen Bilder erst bei gewissen voreingestellten Ereignissen, wie Feuer oder Bewegung von Objekten einer bestimmten Größe erfolgt.

Generell werden die Videos und Bilder im Storage, in sogenannten Ringspeichern abgelegt, die sich je nach Kapazität und Einstellung nach einer gewissen Zeit selbst überschreiben. Hier werden ohnehin nur bei Bedarf Aufnahmen herausgenommen und gesichert. Andere Lösungen, die zum Beispiel im Einzelhandel Bewegungsmuster der Kunden im Ladenlokal aufzeichen und automatisch noch viele andere Statistiken mehr erstellen können, anonymisieren und abstrahieren diese so, dass hier ohnehin keine realen Bilder aufgehoben werden müssen.

Auch vor Fremdeingriffen werden die Systeme mittlerweile maximal geschützt. So muss zum Beispiel direkt nach der Installation der Dahua-Kameras für jede sofort ein neues Zugangskennwort erstellt werden, um Schwachstellen wie voreingestellte Standardpasswörter zu vermeiden. Hier ließ sich Dahua bereits vor Inkrafttreten der DSGVO vom TÜV Rheinland beraten und erarbeitete eine umfassende Lösung zur Zertifizierung des Datenschutzes bei Internet of Things-Produkten für verschiedene Dahua-Produkte wie IP-Kameras, Netzwerk-Videorekorder, Software-Plattformen, intelligente Server und vielen weiteren Lösungen.

Ob auf unseren regelmäßigen Veranstaltungen oder in einem unverbindlichen persönlichen Beratungstermin stellen wir Wiederverkäufern, Errichtern oder

auch Endkunden mit größeren Projekten gerne die Produktpalette und technischen Möglichkeiten vor.