

Verwaltungsgericht Regensburg  
Haidplatz 1  
93047 Regensburg

**Az. RN 9 K 19.1061**

In Sachen

**X**

gegen

**Stadt Passau**

erlauben wir uns unsere bisherigen Ausführungen wie folgt zu ergänzen:

Die öffentliche Videoüberwachung birgt zwangsläufig das reale Risiko, dass die gesammelten Daten einem Kreis unberechtigter Personen zugänglich sind oder werden. Die technischen Anforderungen an ein Sicherheitskonzept beim Einsatz von Überwachungskameras verdienen nach Auffassung des Unterzeichners daher eine weitere Veranschaulichung. Daher erlauben wir uns zur praktischen Relevanz der möglichen Sicherheitsprobleme bei öffentlicher Videoüberwachung zwei Beispiele anzuführen. Die Erläuterungen enthalten keinerlei Implikationen für konkrete Sicherheitslücken bei der Beklagten, sollen aber die Anforderungen an ein umfassendes und praxistaugliches Sicherheitskonzept und seiner Umsetzung veranschaulichen.

Unter dem Link

<http://ip-193-46-68-18.eltronik.net.pl/view/view.shtml>

lässt sich derzeit beispielsweise ein polnischer Marktplatz mit einer Dome-Kamera beobachten.

Unter dem Link

<http://87.54.59.228/view/view.shtml?id=174&imagepath=%2Fmjpg%2Fvideo.mjpg%3Fcamera%3D1&size=1>

kann man den Flughafen Bronholm in Dänemark beobachten.

In beiden Fällen sind sämtliche Bedienelemente verfügbar. Der Betrachter kann also die Kamera schwenken, den Zoom verändern sowie die Lichtempfindlichkeit des optischen Sensors einstellen. Diese Kameras sind dabei für jedermann offen über das Internet zugänglich.

Für dieses Problem lassen sich mit Leichtigkeit unzählige weitere Beispiele finden, von „Webcams“ an Computern, Videokameras an Auto-Raststätten, Mautstationen, in Gondeln oder an Straßenkreuzungen. Denn solche Videokameras, aber auch andere Geräte, können unproblematisch in entsprechenden Suchmaschinen gefunden werden, wobei

<https://www.shodan.io/> die Bekannteste sein dürfte. Mit diesen lassen sich (freiwillig oder unfreiwillig) mit dem Internet verbundene Endgeräte finden.

Dieser Zugriff über das Internet ist im Regelfall darauf zurückzuführen, dass bei der Installation und Einrichtung der entsprechenden Hardware grundlegende Sicherheitsaspekte unbeachtet geblieben sind. Dies betrifft zum Beispiel die erforderliche Änderung der Zugangsdaten, die vom Hersteller vorgegeben sind, oder die unsachgemäße Verbindung des jeweiligen Geräts mit einem Intranet oder dem Internet.

Selbst wenn allerdings die Einrichtung nach dem Stand der Technik erfolgt, so ist damit keineswegs jedes zukünftige Risiko ausgeschlossen. Denn mit fortschreitender technischer Entwicklung muss die Sicherheit angepasst werden.

Zudem können Sicherheitslücken, wie sie in jeder Soft- und Hardware zu finden sind, es Dritten ermöglichen, trotz dieser Vorsichtsmaßnahmen auf die Hardware (beispielsweise in Form einer Dome-Kamera) zuzugreifen und sie umfassend zu steuern. Eine Sicherheitslücke die das ermöglicht ist, wie im vorherigen Schriftsatz ausgeführt, auch bei den im Klostergarten eingesetzten Kamera-Modellen vor Kurzem entdeckt worden. Dass solche Sicherheitslücken bestehen und ausgenutzt werden, kann auch die beste technische Wartung nicht ausschließen.

Bei diesen Aspekten handelt es sich keineswegs um rein akademische oder theoretische Probleme. IT-Fachleute warnen deshalb davor, dass die Installation einer Videoüberwachung immer das Risiko birgt, dass unberechtigte Dritte auf die Daten zugreifen können.