CyOne Security AG

Mini-Drohnen: Cyber-Risiken mindern

Mini-Drohnen sind im Kommen, auch in der Schweizer Armee und Polizeiorganisationen. Mit ihnen steigen die Sicherheitsrisiken – unter anderem aufgrund der Kommunikation über Mobilfunk oder WLAN, aber auch wegen intransparenter Lieferketten.

Mit der Anschaffung der ersten Mini-Drohnen hat die Schweizer Armee 2015 rüstungstechnisches Neuland betreten. Mittlerweile wurden vier Typen beschafft, die unterschiedlicher nicht sein könnten: 33 Gramm wiegt die kleinste, 10 Kilogramm die grösste. Sie alle liefern Bildinformationen im bodennahen Einsatzgebiet, doch ihr Einsatzzweck ist höchst unterschiedlich.

Bildquelle: © VBS/DPPS – Dominic Wenger

Rege Nutzung trotz Sicherheitsrisiken

Nicht nur in der zunehmend mobil vernetzten Armee kommen die kleinen Flugroboter verstärkt zum Einsatz. Auch die Polizei setzt sie immer häufiger ein, etwa bei Suchaktionen. Im zivilen Bereich haben Mini-Drohnen ebenfalls grosses Potenzial, zum Beispiel für Wartungsarbeiten an Stromnetzen.
Trotz steigender Verbreitung sind die Sicherheitsbedenken in der Regel gering. Denn längst nicht alle Anwender sind sich bewusst, dass Mini-Drohnen Ziele für Cyber-Kriminelle sind. Die Verbindung zwischen Drohne und Steuerung erfolgt in der Regel über WLAN oder Mobilfunk – und diese Funknetze bergen Sicherheitsrisiken. Nicht selten sind die Übertragungswege ungenügend geschützt. Zudem werden im militärischen Einsatz Aufklärungsdaten für Führungssysteme bereitgestellt – somit bestehen Schnittstellen zu äusserst sicherheitssensitiven Bereichen.

Intransparenz bei Lieferketten birgt Gefahren

Ganz grundsätzlich gilt: Augen auf beim Drohnenkauf. Die Lieferketten der verbauten Komponenten sind in aller Regel intransparent. Häufig kommen Standardkomponenten aus Asien zum Einsatz, die mit Blick auf die Sicherheit kritisch sein können. Oft sind die Eingriffsmöglichkeiten des Herstellers und damit auch anderer Parteien umfangreich und nicht transparent. Dies zeigt sich momentan im Ukraine-Krieg.
Die Folgen von Sicherheitslücken sind gravierend. So können zum Beispiel Aufklärungsdaten wie Videostreams abgefangen oder bestimmte Standorte (sowohl der Drohne als auch des Piloten) ermittelt werden. Auch denkbar sind Manipulationen an Steuerungs- und Aufklärungsdaten. Oder das sogenannte «Jamming» der Drohne, bei dem der Flugkörper mittels Störsender zum Absturz gebracht wird.
Organisationen sind gefordert, die Cyber Security in Zusammenhang mit der Supply Chain von eingesetzten Drohnen sicherzustellen. Das betrifft sowohl das Drohnensystem als auch IT-Systeme und Schnittstellen bei der Weiterverarbeitung und Bereitstellung der Daten. Hier spielt die Segmentierung respektive Trennung in Zonen eine entscheidende Rolle. Je nach Einsatzszenario können beispielsweise die Steuerungskommunikation und das Videostreaming unterschiedliche Schutzziele haben. Eine mögliche Lösung, dem gerecht zu werden, ist der Hardware Security Anchor. Dieser ermöglicht eine sichere und resiliente Kryptografie für Data at Rest und Data in Transit.
Als kompetenter Schweizer Partner mit langjähriger kryptografischer Expertise in der Entwicklung von Hardware und Software bietet die CyOne Security Unterstützung bei der Umsetzung sicherer Kollaborationslösungen und Zonenübergänge in Drohnen-Backendsystemen.

Erfahren Sie mehr über die IoT Security Solutions für Schweizer Behörden.

Reto Amstad
Senior Security Consultant
Tel. +41 41 748 85 16
reto.amstad@cyone.ch
www.cyone.ch