SICHERHEITSTECHNOLOGIE FÜR DEN LUFTRAUM

– Leitfaden für Käufer

Dedrone

SICHERHEITSTECHNOLOGIE FÜR DEN LUFTRAUM

– Leitfaden für Käufer

Die Drohnentechnologie wird stetig weiterentwickelt, und die Anwendungsmöglichkeiten für Drohnen werden immer vielfältiger und kreativer. Goldman Sachs prognostiziert eine Marktchance für Drohnen von 100 Milliarden Dollar bis zum Jahr 2020. Wie bei jeder Technologie finden die Menschen Wege, um mit Drohnen Probleme zu lösen – gleichzeitig aber auch Möglichkeiten, sie für kriminelle Zwecke zu missbrauchen.

Die Luftraumsicherheitsindustrie wächst schnell, und Gesetze, die die sichere Integration von Drohnen in den nationalen Luftraum regeln, holen nur langsam auf. Angesichts einer steigenden Zahl von Vorfällen mit Drohnen müssen Organisationen mit einer sensiblen, hochwertigen Infrastruktur ihren Luftraum proaktiv vor Gefahren durch Drohnen schützen.

Es ist heute wichtiger als je zuvor, Aktivitäten im Bereich des unteren Luftraums zu verstehen und zu bewerten und ein Bewusstsein für Drohnen zu entwickeln, die in den kritischen Luftraum eindringen.

In diesem Leitfaden erhalten Sie Antworten auf folgende Fragen:

- Wie ermittle ich meinen Bedarf an technischen Lösungen für die Luftraumsicherheit?
- Wer sollte in den Kauf einer Lösung zum Schutz vor Drohnen eingebunden sein?
- Wie läuft dieser Prozess ab?

Inhaltsverzeichnis

1.
Definition von „Luftraum-Sicherheitstechnologie“ und Terminologie

IN DIESEM ABSCHNITT:

- Was ist Luftraum-Sicherheitstechnologie?
- Welche Arten von Informationen stellt Luftraum-Sicherheitstechnologie zur Verfügung?
- Was kann ich gegen Bedrohungen durch Drohnen tun?

Um Drohnen zu identifizieren und zu klassifizieren und die Koordinaten der Drohne sowie des Piloten zu ermitteln, kann eine Kombination aus Hard- und Software verwendet werden. Je nach Art der Hard- und Software können Sie den Drohnenhersteller, das Modell, den Zeitraum der Drohnenaktivität und den Standort des Piloten bestimmen.

Luftraum-Sicherheits-Hardware:
Die Hardware sammelt Daten und Informationen über die Drohne und wird außen in Bereichen installiert, die vor Bedrohungen durch Drohnen geschützt werden müssen.

- **Radiofrequenz-Sensoren:** RF-Sensoren sind die Eckpfeiler der Luftraumsicherheit. Sie entdecken kommerzielle, Hobby- und selbstgebaute Drohnen, ermitteln deren Flugbahn und lokalisieren die Drohne sowie den Standort des Piloten. RF-Sensoren sind in der Lage, den Typ bzw. das Modell der verwendeten Drohne zu bestimmen – wichtige forensische Daten, wenn rechtliche Schritte gegen die Piloten eingeleitet werden sollen.

- **Kameras:** Kameras verfolgen die Bewegungen der Drohne, tragen zur Identifizierung der Ladung bei und zeichnen kriminaltechnisch relevantes Beweismaterial zu eindringenden Drohnen auf.

- **Radar:** Wenn ihre Nutzung erlaubt ist, bieten Radare eine Detektion auch auf große Entfernungen, einschließlich Positionsermittlung der Drohne.

- **Akustische Sensoren:** Drohnen erzeugen charakteristische „Summgeräusche". Akustische Sensoren können diese Tonsignaturen erkennen.

Luftraum-Sicherheits-Software:
Die Software verknüpft Sensoren, führt Analysen auf der Grundlage von maschinellem Lernen durch und ist so etwas wie das zentrale Nervensystem der gesamten Lösung.

- **Benutzeroberfläche:** Die Benutzeroberfläche muss die Anforderungen der Enterprise-Klasse erfüllen, Mehrbenutzerzugriff ermöglichen und eine Meldung ausgeben, sobald sich eine Drohne nähert. Zusätzlich sollten automatisch zusammenfassende Berichte erstellt werden, um Nutzern bei Bedarf unkomplizierte Analysen der wichtigsten Sicherheitsdaten für den Luftraum zu liefern.

- **Videoanalysen:** Videoanalysen mithilfe von IP-Videokameras ermöglichen eine Unterscheidung zwischen sich bewegenden Objekten wie Flugzeugen, Autos, Hubschraubern oder Drohnen.

- **Plattform für maschinelles Lernen:** Eine Software für die Drohnenerkennung muss - ähnlich wie eine Software zum Schutz vor Viren oder Malware - ständig dazulernen und sich aktualisieren.

„Entkoppelte“ Systemarchitektur:
Jede Komponente innerhalb Ihrer Infrastruktur zur Drohnendetektion sollte eigenständig sein. Man spricht bei diesem Prinzip auch von Sensor-agnostisch. Es muss gewährleistet sein, dass verschiedene Marken, Modelle oder Hersteller mit der Drohnenerkennungssoftware kompatibel sind, damit Sie eine kosteneffiziente, flexible und an Ihre Bedürfnisse angepasste Lösung erhalten.

Gegenmaßnahmen und Abwehrtechnologie:
Diese Technologie sammelt keine Daten. Dennoch stellt sie im Rahmen einer Lösung für Luftraumsicherheit eine wichtige Komponente dar. Gegenmaßnahmen können passiven oder aktiven Charakter haben. Mittels Detektionstechnologie wird zunächst die Drohne identifiziert und lokalisiert. Dann kann eine Gegen- oder Abwehrmaßnahme eingeleitet werden.

- **Passive Gegenmaßnahmen** greifen nicht in die Drohnenaktivitäten ein. Zu solchen passiven Maßnahmen gehören etwa das Schließen von Jalousien, die Verlagerung zu schützender Güter oder eine zeitweise Unterbrechung von Betriebsabläufen.

- **Aktive Gegenmaßnahmen** sind für Unternehmen und Individuen normalerweise illegal, da die Beschädigung oder Störung einer Drohne in vielen Ländern eine Straftat darstellt. Ausnahmen können allerdings vorliegen, wenn Drohnenübergriffe nationale Verteidigungsinteressen berühren. Das Militär darf ggf. aktive Gegenmaßnahmen ergreifen und Technologien wie Jam-mer oder Laser gegen Drohnen einsetzen, wenn es angegriffen wird oder seine Sicherheit bedroht ist.

2.
Bedarfsanalyse

IN DIESEM ABSCHNITT:

- Muss meine Organisation Anlagen vor Bedrohungen aus dem Luftraum schützen?
- Was sind meine Ansprüche an und Ziele für ein Luftraum-Sicherheitsprogramm?

Angesichts der steigenden Zahl von Drohnen in unserem Luftraum müssen wir über eine Art Zaun zum Schutz vor Gefahren aus der Luft nachdenken. Für die folgenden Einrichtungen oder Szenarien können entsprechende Sicherheitsvorkehrungen erforderlich sein:

- **Arenen/Stadien:** Schutz von Sportlern und Zuschauern vor physischen Bedrohungen; Schutz von Übertragungs- und Urheberrechten vor nicht zugelassenen Kameras
- **Unternehmen:** Schutz von Rechenzentren, die von Kühlanlagen auf Dächern abhängig sind; Schutz sensibler IT-Infrastrukturen vor Hackerangriffen; Schutz von Prototypen/geistigem Eigentum
- **Justizvollzugsanstalten:** Schutz vor Schmuggel von Waffen, Drogen usw.
- **Bedeutende politische oder gesellschaftliche Ereignisse:** Schutz der physischen Sicherheit größerer Menschenmengen und VIPs vor Paparazzi oder Terroristen

- **Kritische Infrastruktur:** Schutz von Kraftwerken, Öl- und Gasraffinerien, Staudämmen und anderen Versorgungsanlagen, die leicht und unauffällig durch Drohnen gefährdet werden können

Wie sieht Ihr aktueller Sicherheitsbedarf aus?

Drohnen bergen Risiken für die physische und die Cyber-Sicherheit. Drohnen können Hunderte Kilogramm schwere Lasten unterschiedlichster Art tragen. Kameras können für Spionagezwecke verwendet und Waffen, Drogen und andere sensible Ladungen abgeworfen werden. Drohnen sind unter anderem so etwas wie fliegende Laptops. Geschickte Hacker können mit ihnen spionieren oder Rechenzentren und IT-Netzwerke stören.

Gibt es in Ihrem Luftraum unbefugte Drohnen?

Ohne den Einsatz von Technologie ist es sehr schwer, die Situation im Luftraum zu erfassen und zu bewerten. Drohnen bewegen sich schnell und sind mit bloßem Auge oft kaum auszumachen. Auch spezialisierte Sicherheitskräfte haben nur begrenzte Mittel und Möglichkeiten. So können ein eingeschränktes Sichtfeld oder Sichtbehinderungen bei schlechtem Wetter dazu führen, dass schnell fliegende, unauffällige Drohnen selbst von sehr aufmerksamen Personen nicht bemerkt werden.

Verfügt Ihre Organisation bereits über ein Drohnenprogramm?

In einer Reihe von Branchen werden Drohnen zunehmend für Zwecke wie Überwachung, Inspektion, Lieferungen oder Unterhaltung eingesetzt. Es ist wichtig, zwischen solchen autorisierten Einsätzen und nicht genehmigten Drohnen zu unterscheiden, damit der Betrieb reibungslos läuft und das bestehende Drohnenprogramm sicher funktionieren kann.

Was sind Ihre Ziele?

Vielleicht möchten Sie Schmuggelaktivitäten unterbinden, Spionagedrohnen orten oder Anlagen vor physischen Angriffen schützen? Möglicherweise wollen Sie auch einfach Daten zu Bewegungen in Ihrem Luftraum sammeln, um sicherzustellen, dass während bestimmter Vorgänge nichts am Himmel ist. Definieren Sie für sich, was ein effektives Sicherheitssystem für den Luftraum leisten muss.

Beispiele:

- Mehr eingedrungene Drohnen orten und Spione fassen
- Schwachstellen an Anlagen und Gebäuden identifizieren, um sie wirksam gegen Spionage und Störungen zu schützen
- Programme für die Perimeter-Sicherheit strategisch voranbringen
- Schmuggellieferungen unterbinden, bevor sie den Adressaten erreichen

Mithilfe dieser Informationen lassen sich die Werkzeuge bestimmen, die Sie brauchen, um Ihre Ziele zu erreichen.

3.
Erste Schritte

IN DIESEM ABSCHNITT:

- Was brauche ich, um ein Drohnen-Detektionsprogramm zu implementieren?
- Wer sollte an diesem Prozess mitwirken?
- Worauf sollte ich achten, wenn ich verschiedene Technologien prüfe?
- Welche Bedrohungsstufe habe ich und wie dringend ist die Einführung eines Drohnen-Detektionsprogramms?

Informieren Sie Ihre Teammitglieder über die Recherchen und ihre Rolle im Prozess.

Es ist wichtig, dass sowohl die Mitglieder des Sicherheitsteams als auch die Führungskräfte umfassend über Bedrohungen aus der Luft informiert werden. Darüber hinaus ist es aber auch sinnvoll, das IT- und das Facility-Management-Team mit ins Boot zu holen, um eine reibungslose Integration und langfristigen Erfolg zu gewährleisten.

- **Security:** Diese Gruppe umfasst die an der Umsetzung eines Drohnenerkennungsprogramms unmittelbar Beteiligen. Entscheidungsträger wie CSO und CISO gehören ebenso dazu, wie die Personen, die vor Ort für die Sicherheitsaktivitäten zuständig sind und auf Bedrohungen durch Drohnen reagieren müssen.

- **IT:** Die Mitglieder dieses Teams helfen Ihnen zu verstehen, welche Anforderungen hinsichtlich Strom und Konnektivität für das Programm zur Drohnenerkennung erfüllt werden müssen und wie die aus der Drohnenaufklärung gewonnenen Informationen mit anderen Programmen vernetzt werden können. Dieses Team kann auch am Installationsprozess beteiligt sein.

- **Betriebsführung/Facility-Management:** Vom Standort-Management bis zum Hausmeister haben die Mitglieder dieses Teams besonders gute Kenntnisse über die Gegebenheiten vor Ort und können dazu beitragen, die optimalen Standorte für verschiedene Sensoren zu identifizieren.

- **Finanzen/Beschaffung:** Klären sie die Höhe des verfügbaren Budgets und geben Sie alle Details an, die für die Beauftragung eines neuen Anbieters erforderlich sind.

Beurteilen Sie Ihre Technologie-Optionen

Die Luftraumsicherheit ist ein wachsender Markt. Es ist wichtig, eine Lösung vor dem Kauf zu beurteilen und sicherzustellen, dass sich die zugrunde liegende Plattform auf Ihre Bedürfnisse abstimmen lässt. Die technische Lösung muss folgende Bedingungen erfüllen:

- **Bewährt bei verschiedenen Kunden:** Eine einfache Recherche sollte zeigen, ob Ihr Technologieanbieter unterschiedliche Referenzkunden hat, die die Lösung bereits nutzen. Sie sollten das Technologieunternehmen kontaktieren und Informationen über die Erfahrungen mit dem Produkt erhalten können.

- **Skalierbar und zukunftssicher:** Die Technologie Ihrer Wahl sollte die Möglichkeit bieten, später auf einen größeren Schutzbereich ausgeweitet zu werden. Außerdem sollten alle Software-Komponenten regelmäßig aktualisiert werden und in der Lage sein, anhand neuer, am zu schüt-zenden Standort gesammelter Daten zu lernen. Es gibt nicht die eine passgenaue Universallösung. Ihr Erkennungsprogramm sollte sich ständig weiterentwickeln und wie eine Machine-Learning-Plattform oder eine Anti-Virus-Software selbstlernend sein.

- **Enterprise-Klasse:** Unternehmenskunden brauchen Lösungen, die Sicherheitsstandards erfüllen, mit bestehenden Verfahren und Systemen kompatibel sind und ein bedarfsgerechtes Mehrbenutzer-Management ermöglichen.

- **Automatisiert und sofort einsetzbar:** Sie sollten für Ihr Luftraum-Sicherheitssystem keinen speziellen Monitor brauchen. Die Detektionsanalyse sollte unmittelbar verfügbar sein und es dem Sicherheitspersonal ermöglichen, Bedrohungen durch Drohnen zu bewerten und zu analysieren.

- **Ein mehrschichtiges, Sensor-agnostisches Sicherheitsprogramm:** Verschiedene Detektionstechnologien sollten zusammengeführt werden, um ein komplettes System zu schaffen – einschließlich unter anderem akustischer Sensoren, Kameras, RF/WiFi und Radar. Jede Detektionstechnologie bietet zusätzliche Datenschichten und Sie sollten in der Lage sein, eine Vielzahl von Sensor-Marken, -Herstellern und -Modellen zu integrieren, um Ihren Bedürfnissen gerecht zu werden.

- **Intuitiv und leicht in Standard-Betriebsprozesse zu integrieren:** Die Benutzeroberfläche muss einen übersichtlichen Aufbau für Benutzer verschiedener Stufen aufweisen.

- **Kosteneffizient:** Die Einstiegskosten für ein neues Technologieprogramm sollten keine Hürde darstellen. Die Detektionstechnologie sollte in Ihr Budget passen und Raum bieten, Ihr Luftraumsicherheitsprogramm mit der Zeit auszuweiten, wenn Sie mehr über die Aktivitäten in Ihrem Luftraum wissen.

Bestimmen Sie Ihre Bedrohungsstufe:
Ernst: Ihre Organisation war einer Bedrohung ausgesetzt, oder Drohnen befinden sich derzeit in Ihrem Luftraum und gefährden Ihre Sicherheit. Das schließt diejenigen ein, die kritische Infrastrukturen schützen, bei denen ein Offline-Status infolge einer Luftraumverletzung katastrophale Auswirkungen haben kann.

Hoch: Ihre Organisation hat Drohnen in ihrem Luftraum festgestellt und entwickelt aktiv Sicherheitsprotokolle. Drohnenerkennung ist notwendig, um mehr Informationen über die Drohnenaktivitäten zu gewinnen, als Basis für Maßnahmenpläne und Reaktionen. Das gilt beispielsweise für Stadien, die Drohnen über Spielen gesehen haben, oder Gefängnisse, die bereits per Drohne gelieferte Schmuggelware abgefangen haben.

Vorsicht: Ihre Organisation ist sich der von Drohnen ausgehenden Gefahren bewusst, hat aber in ihrer unmittelbaren Umgebung noch keine unbemannten Fluggeräte beobachtet. Drohnendetektion wird dabei helfen, Ihre Risiken zu bewerten. Das könnte beispielsweise Veranstalter betreffen, die ihre Sicherheitskonzepte ausweiten möchten, oder ein Unternehmen, das geistiges Eigentum schützen will.

Niedrig: Ihre Organisation ist sich bewusst, dass Drohnen ein Problem darstellen können, kennt dabei aber noch nicht die konkreten Risiken. Sicherheitsteams möchten möglicherweise auch ein System zur Detektion von Drohnen einführen, um beim Einsatz von Drohnen auf dem Gelände zwischen genehmigten und feindlichen Flugobjekten zu unterscheiden.

Legen Sie Ihr Budget und Ihren Zeitplan fest:

Je nach Bedrohungsstufe müssen Sie festlegen, wie viel Sie in Hardware, Software-Lizenzen und andere Posten investieren können. Möglicherweise müssen Sie sofort einen Kauf tätigen. Klären Sie dies zu Beginn des Prozesses um sicherzugehen, dass Ihr Budget dem Bedarf entspricht.

Bei der Zeitplanung müssen Sie unter anderem folgende Meilensteine berücksichtigen:

- **Recherche und Einstieg:** Reservieren Sie Zeit für die Recherche nach passen-den Lösungen und erste Treffen mit Technologieanbietern.
- **Interner Einkaufszyklus:** Klären sie frühzeitig, wie der in Ihrem Unternehmen einzuhaltende Genehmigungsprozess für Einkäufe aussieht und welche Informationen Sie im Vorfeld brauchen, um einen reibungslosen Einkauf zu gewährleisten.
- **Beschaffung und Produktion von Sensoren:** Möglicherweise müssen Sie zusätzliche Hardware von Drittanbietern beschaffen oder auf die Produktion neuer Hardware warten. Der jeweilige Lösungsanbieter kann Sie zur zeitlichen Planung beraten.
- **Installation und Schulungen:** Abhängig von der Komplexität Ihrer Installation kann es erforderlich sein, dass der Lösungsanbieter Ihren Standort besucht. Sie müssen außerdem Zeit für Installation, Kalibrierung und Tests einplanen, bevor Ihr System voll einsatzfähig ist.

Wenn Sie Kontakt mit einem Technologieanbieter aufgenommen haben, können Sie diese Punkte klären um sicherzustellen, dass der Start des Drohnen-Detektionsprogramms Ihrer Bedrohungsstufe und anderen Anforderungen entspricht.

4.
Beauftragung eines Technologieanbieters

IN DIESEM ABSCHNITT:

- Was sollte ich von einem Technologieanbieter erwarten, wenn ich bereit bin zu kaufen?
- Welche technischen Informationen sollte ich während des Kaufprozesses erhalten?

Wenn Sie bereit sind, einen Technologieanbieter zu beauftragen, sollte dieser auf Ihre Fragen eingehen und in der Lage sein, Sie unverzüglich beim Kaufprozess zu unterstützen. Ein Technologieanbieter sollte Sie ebenfalls mit einigen einführenden Materialien versorgen, einschließlich:

- **Schulungs- und Einführungsmaterialien:** Sie müssen zum Beispiel die Möglichkeit erhalten, sich für Webinare anzumelden, Videos anzusehen oder Handbücher zu lesen.
- **Referenzmaterialien und Forschung:** Der ausgewählte Technologieanbieter sollte Ihnen Zugang zu Informationen verschaffen (zum Beispiel White Papers, Blog-Artikel oder Jahresberichte).
- **Erfolgsgeschichten:** Stellen Sie sicher, dass der Technologieanbieter Fallbeispiele vorlegen kann, aus denen hervorgeht, wie die angebotene Lösung Probleme von Organisationen wie der Ihren lösen kann. Der Anbieter sollte auch in der Lage sein, Kontakte zu Referenzkunden zu vermitteln, die über Erfahrungen mit dem Produkt berichten.
- **Engagiertes Kundenmanagement-Team:** Von der Recherche über die Installation bis zur Wartung sollte das für Sie zuständige Team gut erreichbar sein und klar mit Ihnen kommunizieren.

Bereiten Sie sich auf das Gespräch vor

Möglicherweise verfügt Ihre Sicherheitsinfrastruktur bereits über Sensoren, die in ein Programm für Drohnenerkennung integriert werden können. Darüber hinaus ist es wichtig, vor dem Gespräch die Voraussetzungen der physischen Umgebung zu analysieren und Bedingungen zu berücksichtigen, die spezielle Installationen erfordern. Auch, wenn Sie diese Informationen nicht beim ersten Kontakt mit einem Anbieter brauchen, sollten sie trotzdem beachtet werden, um sicherzustellen, dass Sie ein erfolgreiches Programm entwickeln.

Auf der nächsten Seite finden Sie eine Checkliste für die Suche nach Luftraum-Sicherheitstechnologien. Die darin gesammelten Informationen helfen in Gesprächen mit Technologieanbietern, Ihren Lösungsbedarf zu ermitteln.

Ressourcen-Checkliste:

SENSOR	STANDORT	PRIMÄRE FUNKTION	FABRIKAT/MODELL
IP-Kamera			
Radar			
Akustischer Sensor			
Radiofrequenz-Sensor			
Anderer Sensor			

Technologie-Checkliste:

Überprüfen Sie im Vorfeld, ob Sie die folgenden technischen Voraussetzungen für eine erfolgreiche Bereitstellung erfüllen:

- ☐ Mobilfunkempfang am geschützten Standort (4G-LTE) und/oder Internetverbindung an den Aufstellungsorten
- ☐ Zugängliche Fläche an einer erhöhten Konstruktion für die Anbringung von Sensoren
- ☐ Ein 230-V-Stromanschluss in höchstens 30 m Entfernung vom Installationsort

Checkliste Installationsbereich:

Auch, wenn manche dieser Punkte nicht für Sie gelten, ist es hilfreich, einige Informationen über die Umgebung zu erfassen, die Sie schützen möchten.

- ☐ **Standort:** Städtischer oder ländlicher Standort
- ☐ **Größe der Liegenschaft:** Gebäudehöhen und Dachzugänge
- ☐ **Luftraumbarrieren:** Nähe zu anderen Gebäuden; niedriger oder höher als Ihr Gebäude?
- ☐ **Entfernung zu kritischer Infrastruktur:** z. B. Militärbasen, Rechenzentren, Arenen/Stadien, Gefängnissen, Kraftwerken
- ☐ **Entfernung zu wichtiger Verkehrsinfrastruktur:** z. B. Flughäfen, Autobahnen, Eisenbahnanlagen
- ☐ **Entfernung zu akustischen oder Frequenzsensoren:** z. B. Mobilfunkmasten, Rundfunk-/TV-Sender, DAS
- ☐ **Landschaftsmerkmale:** Offener Raum oder Wald, Hügel/Höhenunterschiede, Entfernung zu Gewässern

ABSCHNITT FÜR NOTIZEN

DEDRONE GMBH
Miramstr. 87
34123 Kassel

Veröffentlicht im Juni 2018

dedrone.com/de

Dedrone