BEILAGE ZUM DSD 3 | 2018

BDSW

INFO
WIRTSCHAFTSSCHUTZ

EINE PUBLIKATION DES ARBEITSKREISES WIRTSCHAFTSSCHUTZ DES BDSW

„Grenzenlose Freiheit“

→ „Über den Wolken muss die Freiheit wohl grenzenlos sein“, so sang Reinhard Mey. Als der bekannte Interpret mit diesem Song Erfolge feierte, gab es Drohnen für den Privatgebrauch noch nicht. Dennoch war es eine textliche Punktlandung, die auch heute noch passt. Denn „grenzenlose Freiheit“, das gilt gerade auch für Drohnen – jene unbemannten Flugkörper – die millionenfach durch die Lüfte ziehen. Grenzen, wie Zäune, Mauern und andere Perimeterschutzsysteme, haben durch Drohnen ihre Schutzwirkung weitestgehend verloren. Sie können einfach oberhalb der Umfriedungen überflogen werden.

Drohnen stellen ein neues Bedrohungsbild dar. Genauso wenig wie Zaungrenzen Hackerattacken verhindern können, kann auch der ausgefeilteste Perimeterschutz keine Angriffe aus dem Luftraum abwehren. Wer dies nicht beachtet, läuft Gefahr, im Zeitalter der Elektronik, der IT und der stürmischen technischen Entwicklung, Palisaden im Stile des Mittelalters zu errichten. Das wäre fatal, denn Unternehmenssicherheit ist nur dann wirklich etwas wert, wenn sie auf aktuelle Sicherheitsherausforderungen adäquat reagiert.

Drohnen oder UAVs (unmanned aereal vehicles), wie sie auf neudeutsch heißen, sind aber nicht nur eine Gefahr. Sie können auch helfen, die Sicherheit von Unternehmen und Bewachungsobjekten entscheidend zu verbessern. So wie Drohnen einen verlängerten Arm von Angreifern darstellen können, können sie auch als „fliegendes Auge“ der Sicherheitsdienste dienen und deren Aufgabenspektrum unterstützen. Drohnen sind aber nicht in der Lage, Streifengänge zu ersetzen, da trotz aller Pluspunkte der elektronischen Visualisierung das menschliche Auge eventuell Veränderungen wahrnimmt, die Kameras verborgen bleiben.

Niemand muss die Befürchtung haben, dass ihn UAVs technisch überfordern. Die gängigen

Ideale Voraussetzungen für einen kriminellen Drohneneinsatz bieten Glasfassaden, wie sie bei vielen Bürogebäuden üblich sind. Foto: Niko Korte / pixelio.de

Modelle arbeiten im teilautonomen Modus – das heißt, sie halten sich automatisch stabil in der Luft. Der Pilot muss lediglich Höhe und Richtung vorgeben, den Rest erledigt eine Art Autopilot. Auch die Landung ist weitestgehend automatisiert. Bricht der Funkkontakt ab, stürzt das UAV nicht etwa ab, sondern geht kontrolliert zu Boden. Der Betrieb einer Drohne erfordert natürlich Grundwissen und Übung, ist aber nicht annähernd so kompliziert und komplex wie der Gebrauch eines herkömmlichen Flugmodells.

Wie die „fliegenden Augen“ im positiven Sinne genutzt werden können, verdeutlicht unser aktueller Hauptbeitrag anhand einiger Beispiele.

Bleiben Sie also auch im Zeitalter der Drohnen auf der sicheren Seite.

Holger Köster
Vorsitzender
BDSW-Arbeitskreis Wirtschaftsschutz ←

„Fliegende Augen“ – ein Einsatzmittel für Sicherheitsaufgaben

Von Klaus Henning Glitza

→ Der Einsatz von Drohnen oder UAVs hat schon längst nicht mehr den exotischen Touch wie noch vor ein paar Jahren. Immer mehr Unternehmen nutzen die „fliegenden Augen“ als Einsatzmittel für Sicherheitsaufgaben und haben nach vorliegenden Berichten gute Erfahrungen damit gemacht.

So setzt die Tochtergesellschaft der Deutschen Bahn AG, die DB Sicherheit GmbH, bereits seit 2014 UAVs ein – für

» Zustands-, Schadens- und Vegetationskontrolle
» Instandsetzung
» Sicherheit und Gefahrenabwehr
» Vermessung

Von „höherer Warte“ aus detektieren die Sicherheitsexperten der Bahn beispielsweise Trampelpfade oder andere Bewegungsspuren, die die Aktivität von Buntmetalldieben und deren mögliche Zwischenlagerstätten offenbaren. Ebenso lassen sich unerwünschte Gegenstände, Tiere oder Personen auf dem Streckennetz und andere Störfaktoren feststellen.

Industriebetriebe und Netzbetreiber wenden UAVs zum Beispiel an, um Pipelines, große Anlagen, kritische Infrastrukturbereiche oder Stromleitungen auf ihren ordnungsgemäßen und störungsfreien Zustand zu inspizieren. Auch bei den Feuerwehren/Werkfeuerwehren ist der UAV-Einsatz längst etabliert. Durch Drohnen kann schnell ein umfassendes Lagebild gewonnen werden. Außerdem ermöglichen UAVs Messungen innerhalb von Rauchwolken, was vom Boden nicht möglich ist.

Einige Sicherheitsdienste nutzen UAVs bereits für die Revierbewachung und für Bereiche, die sehr schlecht einsehbar sind.

Zäune und S-Draht allein schützen nicht mehr vor den Angriffsszenarien der Jetztzeit. Foto: Alexander Dreher / pixelio.de

Generell betrachtet, eröffnen UAVs dieselben Möglichkeiten, die auch ein Helikopter erlaubt, aber mit weitaus weniger Aufwand und ungleich geringeren Kosten. Im Gegensatz zu „Helis“ können UAVs vor Ort vorgehalten werden und sind deshalb zeitnah einsetzbar. Die Polizei setzt aus gutem Grund Hubschrauber bei der Suche nach Tatverdächtigen, Vermissten oder Diebeslagern ein, greift aber aktuell zunehmend auf Drohnen zurück, zum Beispiel in Bayern.

„Helis“ und andere Drehflügler wie Drohnen sind allgemein geschätzt, da sie eine Vogelperspektive ermöglichen. Dieser Blick von oben

» bietet ein ganzheitliches Bild
» erhöht die Sichtweite um ein Vielfaches
» legt Risiken und Schwachstellen offen, die aus Bodensicht nicht ohne weiteres erkennbar sind
» macht Personen, die sich verstecken oder vermisst werden, besser sichtbar
» identifiziert Bodenveränderungen (Hinweise auf vergrabene Gegenstände, z. B. Diebesgut, verbotene Alkoholika oder ein Router, um das WLAN-Netz des Unternehmens „anzuzapfen“)
» lässt oberirdische Verstecke von Gegenständen erkennen.

Welche Einsatzoptionen bieten sich für Sicherheitsdienste?

UAVs können zum Beispiel zur Perimeterüberwachung eingesetzt werden. Einsatztaktischer Nutzwert wäre, dass Drohnenflüge allgemein öfter und kräftesparender durchgeführt werden können als Bestreifungen. Der Einsatz einer Drohne ist immer möglich, ohne dass sich deren Pilot allzu weit von seinem Arbeitsplatz entfernen muss und bedeutet damit den geringsten Eingriff in den Dienstablauf.

Ein ausgezeichnetes Einsatzmittel ist das UAV bei Alarmverifikationen. Zum einen kann es wesentlich schneller am jeweiligen Ereignisort sein und damit schneller zur Klärung eines möglicherweise indifferenten Sachverhalts beitragen. Zur personellen Entlastung führen UAVs bei engen Personallagen – insbesondere dann, wenn nur eine Sicherheitskraft im Einsatz ist.

Wird per UAV eine Straftat entdeckt, ist es möglich, das Unternehmensumfeld nach Täterfahrzeugen, Komplizen etc. abzusuchen bzw. flüchtende Täter zu verfolgen. Als Maßstab ist immer der Datenschutz anzulegen. Ist der Einsatz auf unternehmenseigenem Grundstück unbedenklich machbar, kann das Über-

Ein Multikopter (Drohne mit mehreren Rotoren) steigt auf. Jeder der Rotoren verfügt über einen eigenen Antrieb. Dies sorgt für eine präzisere Steuerung und mehr Stabilität. Mit den noch relativ primitiven UAVs der ersten Jahre haben die heutigen Modelle nur noch wenig zu tun. Foto: Sven Löffler / pixelio.de

Schon eine einfache Jalousie kann vor Ausspähung durch Drohnen schützen. Foto: Cisco Ripac / pixelio.de

fliegen fremder Areale einen Datenschutzverstoß darstellen. Dies muss im Einzelfall geprüft werden.

Mit Drohnen können schließlich Sicherheitskonzepte überprüft oder erweitert werden, indem der Raum oberhalb der Zaungrenze, der ebenso für Angriffe genutzt werden kann, einbezogen wird.

Im Veranstaltungsschutz sind UAVs für den Einsatz von privaten Sicherheitsdiensten nicht erlaubt, da laut Verordnung zur Regelung des Betriebs von unbemannten Fluggeräten ein Betriebsverbot über Menschenansammlungen besteht. Unbedenklich ist dagegen der Einsatz bei der Aufklärung und Absicherung des weitestgehend menschenleeren Veranstaltungsgeländes, um mögliche Vorbereitungs- oder Ausspähhandlungen zu detektieren.

Auch im Personenschutz werden UAVs im rechtlich kompatiblen Maße zur Aufklärung von Objekten, Orten und Wegen eingesetzt. Näher soll auf die Einsatzmöglichkeiten nicht eingegangen werden, um unbefugten Personen keine Anhaltspunkte zu geben.

Über den Zaun steigen? Schnee von gestern im Zeitalter der Drohnen!

Früher mussten Täter Zäune und andere physische Hindernisse überwinden, um auf ein Gelände vorzudringen. Diesen Aufwand, der mit hohen Risiken verbunden ist, haben die UAVs obsolet gemacht. Sie sind die „fliegenden Augen", die jeden Winkel eines Areals erreichen können. Unter günstigen Bedingungen (freie Sicht auf das Objekt) können sie sogar in Gebäude, Hallen oder bei offenen Fenstern in Büros fliegen. Eine Gefahr aus dem Nichts: Gerade in Bereichen mit höheren Betriebsgeräuschen sind ihre ohnehin recht leisen Elektromotoren nicht zu hören. Es gibt aber auch bereits UAVs, die von Haus aus einen minimalen Geräuschpegel aufweisen.

Wie diese neue Bedrohung abwehren?

Ständig in den Himmel gucken – das kann niemand. Das würde auch nicht in allen Fällen etwas nützen, da es UAVs gibt, die Vögeln täuschend ähnlich sehen. Nachts hätte es auch wenig Sinn, denn bei Dunkelheit sind Drohnen ohne elektronische Hilfsmittel kaum zu entdecken. Jedoch kann es nie schaden, wenn das Sicherheitspersonal bei Tageslicht oder in der Dämmerung ab und an den Blick auf den Himmel richtet. Für Unternehmen, die sich – keinesfalls billige – Drohnenabwehrsysteme sparen, wäre das die einzige Möglichkeit, etwas mehr Sicherheit zu erreichen.

Denkbar sind aber auch einige technische Veränderungen

- Generell zu empfehlen: Verlegung von sicherheitsrelevanten Bereichen in den Zentralbereich von Gebäuden
- Spannen von (eventuell blickdichten) Netzen über Höfen und Raucherecken
- Jalousien/Rollläden/Fliegengitter vor Fenstern, um das Eindringen von Drohnen und die Einblickmöglichkeiten zu erschweren
- Änderungen an Gebäudeöffnungen (z. B. Hauben oder Stahlnetze an Luftansaugvorrichtungen von Klimaanlagen).

Wer mehr Geld in die Hand nehmen will und bereit ist, größere Lösungen umzusetzen, hat die Qual der Wahl. Es hat sich inzwischen eine regelrechte Drohnenabwehrindustrie etabliert. Aus Platzgründen stellen wir nur zwei der Abwehrmöglichkeiten vor. Systeme, die eine fremde Drohne übernehmen, bleiben dabei unbeachtet. Der Grund: In Deutschland stehen die entsprechenden Eingriffsrechte Privaten nicht offen, wie Sebastian Dreyer, Security-Experte des Verbandes Unbemannte Luftfahrt (VUL), bekräftigt.

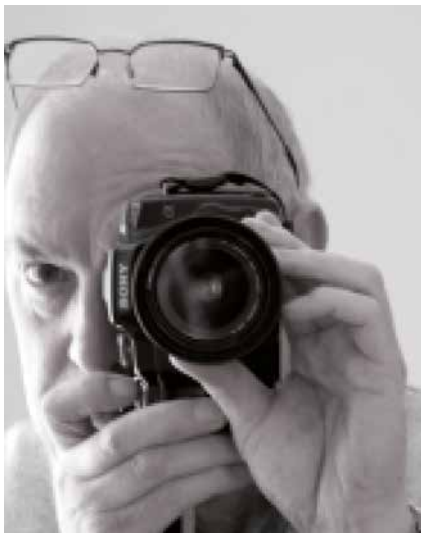
Eine der rechtskonformen Abwehrmöglichkeiten sind Radare im Millimeterwellenbereich, die auch bei Sichteinschränkungen (Nebel, Rauch, Staub) und bei Nacht noch gut funktionieren. Der große Vorteil von Radarsystemen liegt in der Reichweite. Anfliegende Objekte können bereits im Vorfeld weit vor den Grundstücksgrenzen detektiert werden. Durch Analyse des Dopplerspektrums kann dabei auch der Drohnentyp bestimmt werden (welche Klasse, wieviel Rotoren). Dadurch kann das Gefährdungspotenzial besser eingeschätzt werden.

Erkannt werden auch kleinere UAVs, wie Micro- und Mini-UAVs. Allerdings bleiben Nano-Drohnen wegen ihrer noch geringeren Flächigkeit buchstäblich unterhalb des Radars. Eine dieser Zwergdrohnen mit integrierter Kamera misst gerade einmal 4 x 4 Zentimeter. Die Empfindlichkeit einfach zu erhöhen, ist kein gangbarer Weg, da vermutlich zahllose Fehlalarme die Folge wären. Das entwickelnde Fraunhofer-Institut für Hochfrequenzphysik und Radartechnik weist allerdings darauf hin, dass von Nano-Drohnen wegen der geringen Zuladung und Reichweite nur eine geringe Gefahr ausgeht.

Eine weitere Option ist der Einsatz von Sensortechnik. Diese basiert unter anderem darauf, dass keine Drohne ohne Motorsteuerung auskommt, die hochfrequente Geräusche emittiert. Kaum ein UAV kann ohne Funkwellen (Fernsteuerung, Videoverbindung) seinen Kurs fliegen. Diese Indikatoren fallen allerdings bei UAVs weg, die vorprogrammierte GPS-Routen abfliegen und Videosequenzen intern speichern statt sie zu senden.

Der Nachteil von Sensoren ist ihre relativ geringe Reichweite. Drohnenalarm wird meist erst ausgelöst, wenn sich das UAV bereits im relevanten Gebiet bewegt. Blitzaktionen, wie schnelle Fotoserien bzw. rasches Aufnehmen oder Abladen von Gegenständen, geschweige denn Anschläge, können so kaum unterbunden werden. Der Vorteil der Sensoren liegt aber zweifellos darin, dass sie – je nach Empfindlichkeit – auch Nano-UAVs orten können.

Es ist festzustellen, dass es trotz diverser Systeme um eine funktionierende Drohnenabwehr für deutsche Flughäfen nach wie vor schlecht bestellt ist, wie Marian Kortas vom Verband Unbenannte Luftfahrt (VUL) deutlich macht. Nach seinen Angaben habe der Staat Israel speziell für den Flughafen Ben Gurion in Tel Aviv ein gutes System zur Drohnendetektion und -abwehr installiert, das 95 Prozent der handelsüblichen Drohnen (DJI etc.) erkennt. Bei den anderen Systemen reicht wiederum die Reichweite für so große bauliche Anlagen nicht aus. Auf diesem Gebiet besteht also dringender Handlungsbedarf. ←



Einschleusen eines Agenten, um sensible Informationen zu stehlen? Das gehört aufgrund der modernen Drohnentechnik in vielen Fällen der Vergangenheit an.
Foto: Karl-Heinz Laube / pixelio.de

Analysen und Hilfestellungen zum Wirtschaftsschutz

Von Dr. Berthold Stoppelkamp
Leiter des Hauptstadtbüros des BDSW und zuständiges Geschäftsführungsmitglied für den Arbeitskreis Wirtschaftsschutz

VDMA Studie Produktpiraterie 2018

→ Produkt- und Markenpiraterie fügen Unternehmen des deutschen Anlagen- und Maschinenbaus jährlich Schäden von 7,3 Milliarden Euro zu. 2017 waren 71 Prozent der Unternehmen betroffen. Der Umsatz der Schadenshöhe würde knapp 33.000 Arbeitsplätze sichern. Besonders betroffen sind Unternehmen ab 1.000 Beschäftigten. 82 Prozent aller betroffenen Unternehmen gaben an, Opfer von Ideendieben aus der Volksrepublik China geworden zu sein. **www.vdma.org** ←

BKA Bundeslagebild Wirtschaftskriminalität 2017

→ Mit 74.070 registrierten Fällen in 2017 ist die Wirtschaftskriminalität in Deutschland zum Vorjahr um 28,7 Prozent angestiegen. Es wurde ein Schaden von 3,74 Milliarden Euro registriert. Niedrige Zinsen und Digitalisierung bringen neue Formen des Anlagebetrugs hervor. Risikobehaftet sind auch Kapitalanlagen in bestehende virtuelle Währungen. **www.bka.de** ←

Continental verbietet WhatsApp und Snapchat

→ Der Automobilzulieferer Continetal hat seinen Mitarbeitern wegen Datenschutzbedenken aufgrund der EU-Datenschutzgrundverordnung den Einsatz von Social-Media-Apps wie WhatsApp und Snapchat auf Dienst-Handys untersagt. Diese griffen auf persönliche und damit potenziell vertrauliche Daten unbeteiligter Dritter zu. Dies betreffe im Konzern mehr als 36.000 Mobiltelefone. **www.heise.de** ←

KPMG-Studie: Wirtschaftskriminalität 2018

→ Jedes dritte Unternehmen in Deutschland (32 Prozent) war in den letzten zwei Jahren Opfer von Wirtschaftskriminalität. Die häufigsten Deliktarten sind Betrug und Untreue (58 Prozent). Diebstahl und Unterschlagung betreffen im Schnitt 40 Prozent der Unternehmen. Von Datendelikten sind mittlerweile bereits 31 Prozent der repräsentativ befragten 702 Unternehmen betroffen.

www.kpmg.com ←

BDSW

BDSW BUNDESVERBAND DER SICHERHEITSWIRTSCHAFT

Verantwortlich: Dr. Berthold Stoppelkamp
Redaktion: Klaus Henning Glitza

Norsk-Data-Straße 3 · 61352 Bad Homburg
Fon: +49 6172 948050 · Fax: +49 6172 458580

Mail: mail@bdsw.de
Web: www.bdsw.de