FLY ME TO THE DOOM?

DER ANGRIFF VON OBEN

Drohnen bringen Hobbypiloten nicht nur Spaß, sondern übernehmen auch professionelle Aufgaben, von der Vermisstensuche bis hin zum Medikamententransport. Gleichzeitig fordern sie traditionelle physische und Cybersicherheitssysteme heraus, denn diese sind selten auf Angriffe aus der Luft vorbereitet…

Text: **Jörg Lamprecht**

Drohnen sind faszinierend, denn sie befähigen Menschen, an Orte zu gelangen, die sie vorher nicht ohne weiteres erreichen konnten. Die unbemannten Fluggeräte sind Vehikel für Sensoren, Waren und bald auch Menschen. Längst haben sie sich von Spielgeräten für Technikfreaks zu vielseitigen Werkzeugen in den Händen von Profis entwickelt. Laut einer Studie des Bundesverbands der Deutschen Luftverkehrswirtschaft (BDL) und des Bundesverbands der Deutschen Luft- und Raumfahrtindustrie (BDLI) aus dem Februar dieses Jahres sind derzeit rund eine halbe Million Drohnen im deutschen Luftraum unterwegs. 19.000 davon werden für kommerzielle Zwecke genutzt, unter anderem zur Vermessung, Kartierung, Inspektion und für Film- und Fotoaufnahmen. Bis zum Jahr 2030, so die Prognose, wird die Zahl der Drohnen in Deutschland auf 850.000 wachsen, wobei das Wachstum vor allem vom kommerziellen Bereich getrieben wird. Der deutsche Drohnenmarkt wird demnach bis 2030 von 574 Millionen Euro auf fast 3 Milliarden Euro anwachsen, was einer jährlichen durchschnittlichen Wachstumsrate von 14 Prozent entspricht.

SICHERHEITSLÜCKE LUFTRAUM

Die Drohnentechnologie macht rasante Fortschritte: Drohnen, die mehrere Hundert Gramm Traglast transportieren und kilometerweit fliegen können, sind heute für ein paar Hundert Euro zu haben, im Internet oder dem Technik-Markt um die Ecke. Und dank GPS und vorinstallierter Sicherheitsfeatures sind sie auch für Ungeübte leicht zu bedienen. Eben diese Eigenschaften eröffnen auch Kriminellen neue Möglichkeiten. Denn: Herkömmliche Sicherheitssysteme wie Zäune, Videoüberwachung und Zutrittskontrollen sind auf den Boden und die ersten Meter darüber ausgerichtet. Der Luftraum hingegen ist fast immer ungeschützt. Und diese Sicherheitslücke machen sich Drohnenpiloten zunutze.

So haben beispielsweise Gefängnisse weltweit massive Probleme mit Drohnen, die Drogen, Mobiltelefone, Werkzeuge und sogar Waffen unbemerkt in die Einrichtungen schmuggeln, teilweise direkt bis an die Zellenfenster. Doch auch die Sicherheit von Industrieunternehmen und kritischen Infrastrukturen wird zunehmend von Drohnen gefährdet. Der US-amerikanische E-Auto-Hersteller Tesla beispielsweise, hatte mehrfach Probleme mit Drohnen, die im Auftrag ungeduldiger Kunden und Investoren Luftaufnahmen von der Produktionsstätte des begehrten Model 3 machten. Die Stakeholder wollten auf diese Weise mehr über die zunächst schleppende Produktion herausfinden. Apple wiederum kämpfte mit Drohnenpiloten, die Aufnahmen von der Baustelle seines neuen Riesen-Campuses in Kalifornien machten und ins Internet stellten. Das nach den ersten Vorfällen extra eingestellte Sicherheitspersonal konnte dagegen offenbar nichts ausrichten. Ähnlich erging es Facebook beim Bau eines neuen Rechenzentrums in Texas.

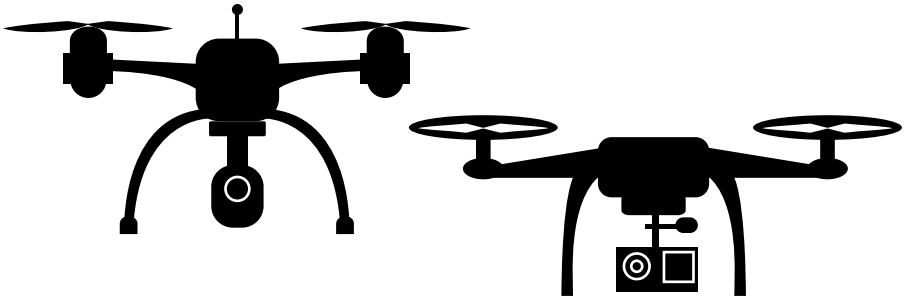
Eine Drohne vor dem Fenster kann leicht die Kommunikation einer drahtlosen Tastatur und die Eingabe von Passwörtern mithören.

Im Juli 2018 ließen Greenpeace-Aktivisten medienwirksam eine Drohne gegen ein französisches Atomkraftwerk fliegen, um dessen Verwundbarkeit zu demonstrieren. Und auch die Betreiber von Umspannwerken, Raffinerien und Pipelines sind beunruhigt, denn Sabotage- oder Terrorakte aus der Luft hätten verheerende Folgen.

DROHNEN KÖNNEN DATEN UND IP STEHLEN

Die Möglichkeiten, mit Drohnen Unternehmen anzugreifen, sind vielfältig. Sie können Mitarbeiter sowie ein- und austretende Personen beobachten, Objekte auf das Betriebsgelände oder von dort nach draußen transportieren, kritische Teile der Infrastruktur wie Lüftung und Kühlung sabotieren, mit hochauflösenden Kameras Dokumente, Produkte oder auch PIN-Eingaben abfilmen und mit entsprechender Technik ausgerüstet, Gespräche abhören.

Auch Angriffe auf das IT-Netz können aus der Luft erfolgen. Mit sogenannten Sniffern ausgestattete Drohnen können drahtlose Infrastrukturen und mobile Endgeräte auskundschaften und eventuelle Sicherheitslücken aufspüren und ausnutzen, sei es im



WLAN, in kabellosen Verbindungen zu Geräten wie Tastaturen oder Druckern, oder in loT- und drahtlosen Building-Management-Systemen. Ein Fortune-500-Kunde des deutsch-amerikanischen Technologieunternehmens Dedrone fand eine Drohne auf dem Dach seines Rechenzentrums. An der Drohne waren ein Sniffing-Gerät, ein Raspberry Pi und ein Transreceiver befestigt. Es ist unwahrscheinlich, dass die Angreifer sich in das Rechenzentrum hacken wollten, da die meisten Rechenzentren nicht über WiFi verfügen. Das Gerät war aber sehr wohl in der Lage zu überwachen, wer das Gebäude wann betrat oder verließ, da es alle drahtlosen Geräte „sehen" konnte. Eine Drohne mit Hacking-Equipment wurde unbestätigten Berichten zufolge auch auf dem Dach des Hauptsitzes von Credit Suisse in Zürich gefunden.

Forscher in Singapur haben 2015 gezeigt, dass sie mit einer Drohne, einem Mobiltelefon und einer App Druckaufträge eines WiFi-Druckers im 30. Stock eines Bürogebäudes abgreifen konnten. In einem anderen Fall haben Forscher aus Kanada und Israel mit einer Drohne eine Lücke in einem Funkstandard ausgenutzt und die Kontrolle über smarte Glühbirnen übernommen. Es gelang ihnen, die Lichter ein- und auszuschalten und die Lampen mit einer Drohne aus einer Entfernung von 350 Metern umzuprogrammieren.

NICHT AUF DEM RADAR

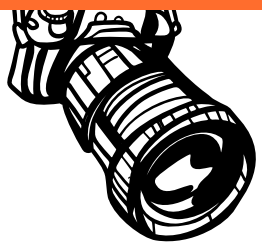
Das Grundproblem besteht darin, dass niemand mit einem Cyberangriff aus der Luft rechnet. Die Reichweite eines Firmenfunknetzes ist begrenzt, sodass man sich innerhalb des Firmengeländes sicher fühlt, erst recht im 30. Stock. Doch Drohnen können unbemerkt innerhalb des Perimeters auf Dächern oder Fensterbänken landen oder auch längere Zeit in der Luft stehen, wo sie kaum zu hören und zu sehen sind. So können sie aus geringer Entfernung die Kommunikation zwischen internen Systemen mitschneiden oder auch manipulieren. Eine Drohne vor dem Fenster kann leicht die Kommunikation einer drahtlosen Tastatur und die Eingabe von Passwörtern mithören.

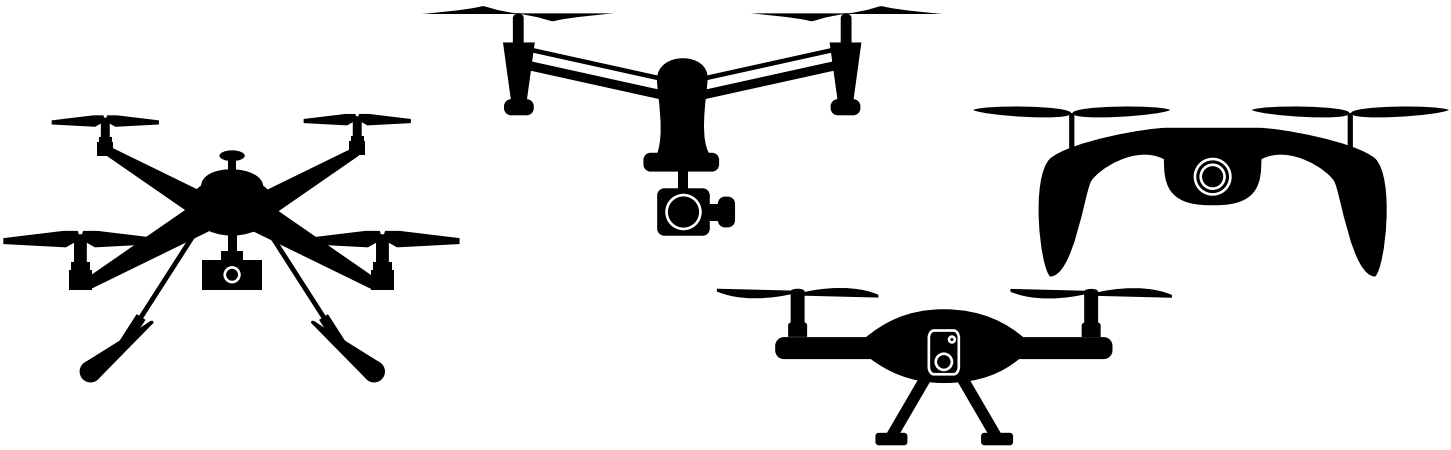
DROHNEN-DETEKTION INTEGRIEREN

Drohnen verbinden physische mit Cyber-Sicherheit, indem Sie Angreifern dabei helfen, bisher unbeachtete Sicherheitslücken im IT-Netz aus der Luft auszunutzen. Immer mehr Unternehmen und kritische Infrastrukturen erweitern daher ihre Sicherheitskonzepte um Technologien zum Schutz vor Drohnen. Dabei bildet ein zuverlässiges Detektions- und Warnsystem, das in bestehende Sicherheitssysteme integriert wird, die Grundlage für alle weiteren Maßnahmen. Denn nur, wenn Drohnen bemerkt werden, kann überhaupt etwas gegen sie unternommen werden.

Für die Kommunikation zwischen Drohne und Fernsteuerung werden spezifische Funkprotokolle verwendet. Spezielle Funkfrequenz-Sensoren, auch RF-Sensoren genannt, sind mithilfe intelligenter Software in der Lage, diese Signale zu erkennen und zu interpretieren. Drohnen werden nicht nur in Echtzeit detektiert, sondern auch Informationen wie Hersteller und Modell sowie die genaue Position und Flugroute ermittelt. Mit hochauflösenden Kameras kann der Drohnenalarm optisch verifiziert und eine mögliche Traglast identifiziert werden. Das Sicherheitspersonal wird bei einer Drohnensichtung umgehend verständigt, sodass sofort Maßnahmen eingeleitet werden können. Ist beispielsweise eine Kameradrohne im Anflug, können Jalousien

Die Möglichkeiten, mit einer Drohne Unternehmen anzugreifen, sind vielfältig.





geschlossen oder Prototypen verhüllt werden. Ist eine Drohne gelandet oder hat sie etwas abgeworfen, kann sie bzw. können die Gegenstände schnell ausfindig gemacht und sichergestellt werden. Besteht der Verdacht eines Angriffs auf das IT-Netzwerk, kann das WLAN abgeschaltet werden.

DROHNEN-RISIKO ANALYSIEREN

Mindestens ebenso wichtig wie das gezielte Handeln während eines Drohnenalarms ist die längerfristige Analyse von Drohnenaktivitäten im überwachten Luftraum und die Ableitung möglicher Aktivitätsmuster. Dazu müssen alle detektierten Drohnenflüge und Informationen wie Drohnenhersteller, -modell, Wochentag, Tageszeit, Flugdauer und Flugroute automatisch dokumentiert und analysiert werden. Ziel ist es, die Motive der Drohnenpiloten zu verstehen, um effektive Vorkehrungen zu treffen. Wird beispielsweise auffällig häufig ein bestimmtes Gebäude angesteuert, gilt es zu überlegen, was dort für den Drohnenpiloten von Interesse sein könnte. Kommen Drohnen nachts, ist dies per se verdächtig, denn nachts ist das Fliegen von Drohnen ohne Genehmigung verboten. Wiederholen sich Flüge zu bestimmten Zeiten, sollte man untersuchen, was im Unternehmen gerade stattfindet und welche Mitarbeiter zu diesen Zeiten vor Ort sind. Diese Informationen sind umso wichtiger, als es privaten Unternehmen und Organisationen nicht erlaubt ist, aktiv in den Luftraum einzugreifen und Drohnen physisch zu stoppen. Technologien wie das Stören der Funk- und GPS-Verbindungen, das so genannte Jamming, dürfen in Deutschland nur von Polizei und Militär eingesetzt werden, da auch andere Frequenzen in der Umgebung beeinträchtigt werden können.

FAZIT

Drohnen werden sich weiter etablieren. Neben allen Vorteilen bringen sie ernstzunehmende Risiken mit sich und machen den Luftraum zur Sicherheitslücke. In den Händen von Kriminellen bedrohen sie die physische und Cyber-Sicherheit von Unternehmen und Organisationen. Diese sollten frühzeitig ihr individuelles Drohnenrisiko ermitteln, Schwachstellen im Sicherheitssystem identifizieren und Vorkehrungen treffen. Entsprechende Lösungen, die Drohnen in Echtzeit detektieren, lokalisieren und sämtliche Daten als Grundlage für wirksame Maßnahmen analysieren, stehen zur Verfügung.

Hier gelangen Sie zur Autorenseite mit thematisch relevanten Empfehlungen von Jörg Lamprecht.

Bild: www.dedrone.com / Jens Distelberg

Jörg Lamprecht

... baute zunächst mit Aibotix den Marktführer für Premium-Drohnen auf, den er 2014 an den Konzern Hexagon verkaufte. 2015 gründete er in Kassel Dedrone, Pionier und Marktführer für Drohnen-Detektion, insbesondere für kritische Infrastrukturen und Unternehmen. Heute hat er 75 Angestellte und Hauptstandort ist San Francisco.

MEHR DAZU

...finden Sie unter:
www.dedrone.com
oder auf dem **European Drone Summit** in Stuttgart am 18./19. September 2019.
Weitere Infos unter:
www.europeandronesummit.eu/de