UAV CyberSecurity
Pentesting Services

SENAIR

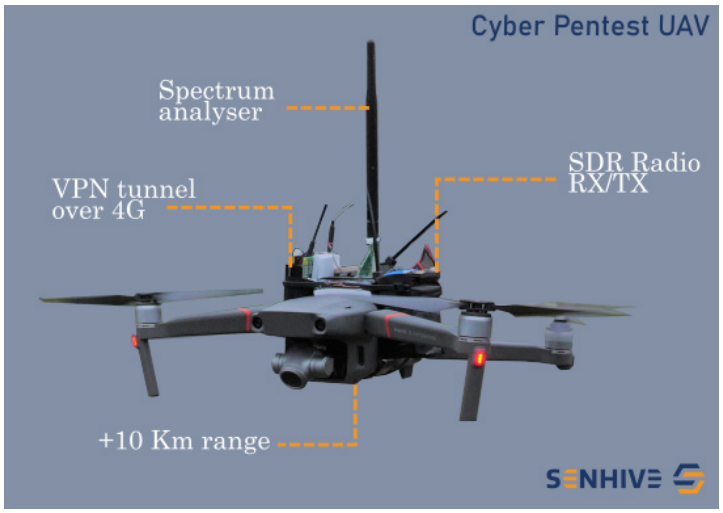
IS JOU IT INFRASTRUCTUUR VEILIG TEGEN DRONES ?

Het beveiligen van kritische infrastructuur stopt vandaag niet meer aan de toegangscontrole of de firewall.
Meer en meer merken we dat drones worden ingezet om via fysieke toegang tot het domein de kwetsbaarheden van de IT infrastructuur bloot te leggen en te omzeilen.

De autonomie van drones en de vooruitgang in draadloze technologie en artificiële intelligentie, laten vandaag toe dat drones ongemerkttoegang kunnen krijgen tot hetbedrijfsnetwerk. (e.g.: een gemiste update van een draadloze printer)

Eenmaal de drone zijn malware heeft geïnstalleerd verdwijnt hij van het toneel en wordt het een uitdaging om via forensisch analyse de oorzaak van de aanval te achterhalen.

Naast de IT infrastructuur worden drones ook vaak ingezet in zogenaamde OSINT operaties (Open-Source Intelligence).
Hierbij probeert een drone via RF spectrum analyse te achterhalen welke frequenties worden gebruikt voor bijvoorbeeld een toeganscontrole, een automatische poort, ... om zich dan te kunnen voorbereiden voor een specifieke aanval op kwetsbaarheden van het gebouw.



Enkele scenarios waar vandaag UAV's reeds worden ingezet tijdens een cyber aanval.

Denial of service
Scenario: een drone landt op het dak van een bedrijfsnetwerk en doet een brute-force attack op een laag beveiligd wifi netwerk, waarna hij via het lokale netwerk zijn aanval verderzet tot een (D) DOS attack

Jamming
Scenario: een drone landt op het dak van een logistiek center. Hij start zijn lokale jammer om interferentie te veroorzaken op de draadloze scanners van de orderpickers. Waarna de hacker "ransomware" vraagt aan het getroffen bedrijf.

Man-in-the-middle
Scenario: een drone landt op het dak van een bedrijfsnetwerk en zet een valse wifi netwerk op onder dezelfde SSID als die van het bedrijf. Een werknemer komt op het valse wifi-netwerk dat wordt omgeleid tot de PC van de hacker, waar deze in kwestie alle traffiek kan onderscheppen en analyseren.

Sen-AIR -SR: Short-Range drone detectie radar

HOE JE TE BEVEILIGEN TEGEN CYBER UAV RISICO ?

Vandaag zijn er reeds tal van sensoren die je een duidelijk luchtbeeld kunnen geven rond kritische infrastructuur. Op basis van topografie, wetgevend kader, en risico niveau kan een counter UAV systeem worden samgengesteld op basis van camera detectie, radar en spectrum analyse....


Sen-AIR -LR: Short-Range drone detectie radar

BEVEILIG JE TEGEN UAV CYBER RISICO 3 STAPPEN

RisicoAnalyse
Via een combinatie van OSINT + intake gesprek identificeren we welke kwetsbaarheden zich kunnen voordoen bij het gebruik van verschillende drone types.

Pentesting
In samenspraak met de klant bepalen we de ROE (rules of engagement) en voeren we een aanval uit met behulp van UAV, spectrum analyzers, jammers, ... met als doel kwetsbaarheden op IT/netwerk niveau te identificeren.

Audit Rapport
Alle kwetsbaarheden en aanbevelingen voor het dichten van beveiligingslekken worden toegelicht gedurende een persoonlijke workshop + audit rapport.

Meer info: www.senhive.com

SENHIVE

The Beacon
Sint-Pietersvliet 7
2000 Antwerpen
Belgium

Droneport
Lichtenberglaan 1090
3800 Sint-Truiden
Belgium