Lähde:
cisa.gov/unmanned-aircraft-systems

Suojaa dronesi

TIETOTURVAA JA -SUOJAA KOSKEVAT OHJEET

Muokkaaja:
Ari Järvinen, Rakennuspooli

Dronet integroituvat nopeasti jokapäiväiseen elämäämme, kuten älypuhelimemme ja tietokoneemme. Kun dronejen suosio kasvaa, niistä voi tulla helppoja kohteita niille, jotka haluavat hyödyntää liitettyjen laitteiden haavoittuvuuksia vaarantaakseen henkilökohtaisen yksityisyytemme.

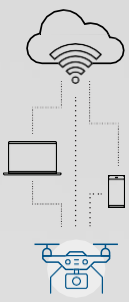
Näissä turvallisuusohjeissa esitetään dronejen käyttäjille vaihtoehtoja tietojensa suojaamiseksi ja tietosuojariskien minimoimiseksi.

Mikä on liitetty laite?

Liitetyt laitteet ovat fyysisiä objekteja, jotka vaihtavat tietoja muiden laitteiden ja järjestelmien kanssa internetin kautta.

Yksityishenkilöt ja organisaatiot käyttävät liitettyjä laitteita ja järjestelmiä päivittäin ympäri maailman. Liitettyjä laitteita ovat mm. kannettavat tietokoneet, älypuhelimet, tabletit, älykkään kodin järjestelmät, autot ja dronet.

Dronet ovat usein yhteydessä Internetiin muiden laitteiden kautta Bluetoothin tai WiFin avulla, joten ne myös altistuvat monille näiden yhteyksien haavoittuvuuksille, joita voidaan hyödyntää kyberhyökkäyksille ja yksityisyyden loukkauksille.



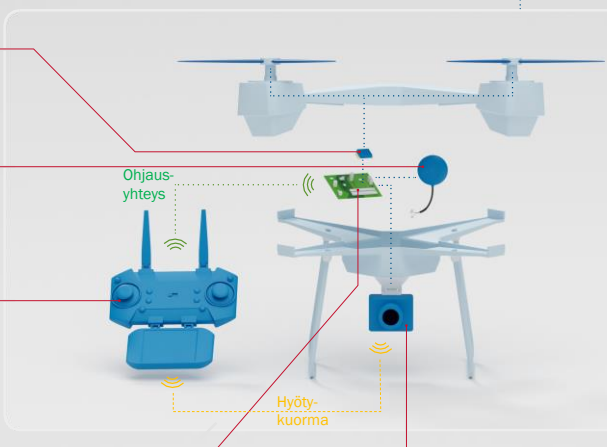
Liitetyt komponentit

Dronekomponentit, jotka keräävät ja välittävät tietoja Internettiin WiFin tai Bluetoothin kautta, ovat alttiita hyväksikäytölle.

Lennättäjä
Lähettää toimintojen, kuten nopeuden säätämiseksi komentoja dronen vastaanottimelle elektronisten signaalien avulla

GPS
Tuottaa paikannussatelliittien signaaleista maantieteelliset koordinaatit, jotka mahdollistavat automaattisen leijutuksen, itsenäisen lennon ja alle 120 metrin lento-korkeuden sekä reittipistenavigoinnin.

Ohjaus- ja hallinta-asema (GCS)
Sisältää ohjelmistoja, jotka mahdollistavat ohjaimen käyttämisen, mukaan lukien reaaliaikaisen videoseurannan (hyötykuorma) ja lentoparametrien välittämisen (ohjausyhteys) dronen ollessa toiminnassa.



Ohjelmisto/laiteohjelmisto
Synkronoi kaikki dronen sisäiset komponentit lähettämällä ohjaimelta vastaanotetut komennot dronen eri fyysisiin komponentteihin. Käyttäjän on päivitettävä ohjelmistot säännöllisesti, jotta dronea voidaan käyttää luotettavasti ja mahdollisimman turvallisesti.

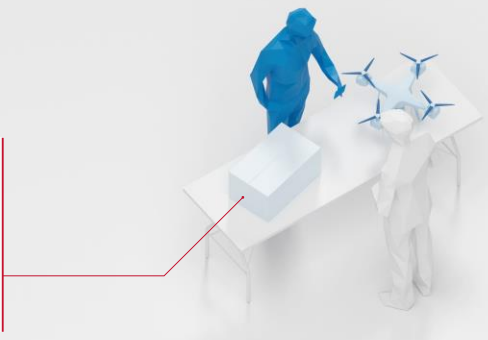
Kamera tai muu hyötykuorma
Lennättämisen videoseuranta (vast.) tai muu hyötykuorma. Data voidaan tallentaa myös paikallisesti muistikortille (vast.).

Droneturvallisuus eri vaiheissa

Tietojen tai yksityisyyden loukkauksen todennäköisyyden vähentämiseksi kaupallisten ja harrastekäyttöön tarkoitettujen miehittämättömien ilma-alusten käyttäjien olisi varmistettava, että heidän laitteensa ja datansa suojataan toiminnan kaikissa vaiheissa.

ENNEN LENTOA

Aloita dronesi turvallisuudesta huolehtiminen jo hankintaa harkitessasi. Huomio seuraavat tietoturvaan ja -suojaan liittyvät suositukset ennen ostopäätöstä ja dronen käyttöönoton yhteydessä.



Dronen ja sen varusteiden ostaminen

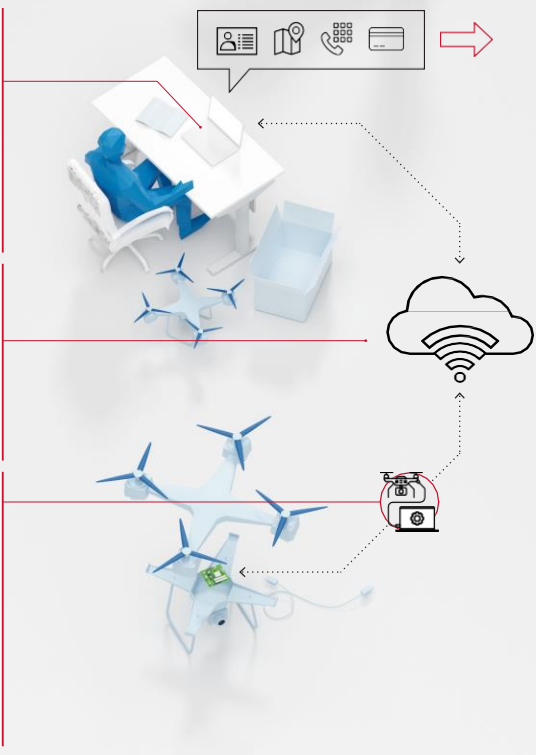
Varo: Drone ja siihen käytetyt kriittiset komponentit lisäävät riskiä, että niiden kautta pääsee luvattomasti käsiksi henkilötietoihisi tai dronen avulla hankkimaasi dataan (kuviin, videoon tms.)

Huomioi:
- Tiedosta, missä dronesi ja sen hyötykuorma (kamera tms.) on valmistettu.
- Käytä aikaa valmistajien tietosuojakäytännön ymmärtämiseen ennen ostamista, mukaan lukien miten ja missä tietosi tallennetaan ja jaetaan jo pelkäästän lupasi perusteella.

Drone-tiin määrittäminen

Varo: Kun rekisteröidyt sovelluksiin, henkilökohtaiset tietosi, mukaan lukien luottokorttitiedot, voidaan tallentaa ja jakaa valmistajan kanssa.

Huomioi:
- Valmistajan rekisteröintivaatimukset ja mitä tietoja voit niiden perusteella kieltäytyä jakamasta.
- Vahvojen salasanojen käyttäminen tileillä ja/tai oletussalasanojen vaihtaminen.
- Monivaiheisen (2FA/MFA) todennuksen käyttö, jos mahdollista.
  - Koodi lähetetään matkapuhelimeesi tai tietokoneeseesi, aina kun dronesi otetaan käyttöön. Ilman oikean koodin syöttämistä dronesi ei toimi.



Yhdistäminen Internettiin tai toisiin laitteisiin

Varo: Drone on etähallittavana laitteena altis rikollisten hakkeroinnille ja kaappauksille.

Huomioi:
- Käytä hyötykuorman yhteytenä vain turvallista Wi-Fi-verkkoa.
- Jos omistat dronen, jossa on käytettävissä LDM (Local Data Mode), niin kytke se päälle estääksesi tietojesi lähettämisen tai jakamisen. Muista, että vaikka sallisit karttapäivitykset LDM:n ollessa aktiivinen, niin pelkkä tieto missä lennätät hyötykuormaa voi olla jollekin arvokas tieto.

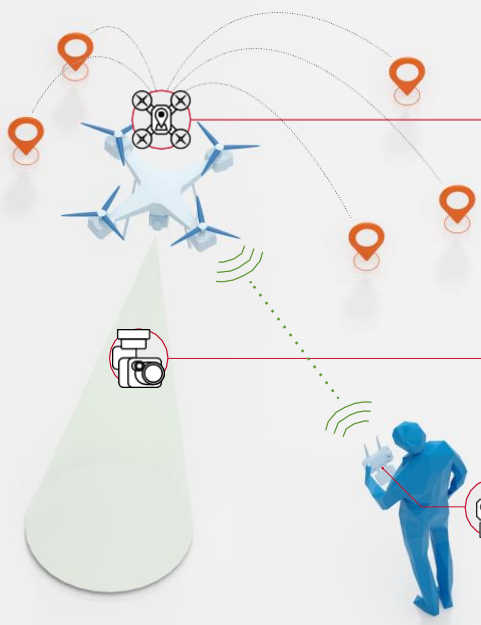
Dronen käyttöön tarvittavien ohjelmistojen ja laiteohjelmistojen lataaminen ja ylläpito

Varo: Dronesi järjestelmä sisältää ohjelmiston ja laiteohjelmiston, jotka synkronoivat kaikki dronen käytön komponentit. Drone ei voi toimia ilman ohjelmistosovelluksia. Hakkerit voivat yrittää manipuloida ohjelmistoa häiritäkseen dronesi toimintaa ja päästäkseen käsiksi sen tietoihin (dataan).

Huomioi:
- Päivitä ohjelmistot säännöllisesti tunnistettujen haavoittuvuuksien korjaamiseksi.
- Lataa ohjelmistot vain käyttäjät todentavista ja yhteyden suojaavilta toimittajien verkkosivustoilta.
- Tarkista käyttöoikeussopimusten mahdolliset muutokset ennen ohjelmiston hyväksyntää.
- Perehdy päivityksen sisältöön ja vaikutuksiin ennen asennusta.

LENNON AIKANA

Nyt kun drone on asennettu, varmista, että kaikki sen komponentit ovat turvallisia lentotoiminnan aikana.



GPS:n hyödyntäminen lennon aikana

Varo: Vaikka dronen lennättäminen onnistuu ilman GPS:ääkin, niin rikolliset voivat vaikuttaa navigointiin ja paikannukseen käytettävään GPS:ään.

Huomioi:
- "Palaa kotiin" (RTH) sijainnin asettaminen helpottamaan dronen talteenottoa.
- Varmistu ja tee tarvittaessa GPS-kalibrointi ennen lentoa.
- Vältä signaalihäiriöiden lähteitä.

Kameran käyttäminen talienteiden tekemiseen lennon aikana

Varo: Kamerat ovat alttiita hakkeroinnille, ja rikolliset voivat päästä lennon aikana käsiksi sen dataan huonosti suojatun hyötykuorman datayhteyden kautta.

Huomioi:
- Käytä kameran linssinsuojusta aina aktiivin toiminnan ulkopuolella..
- Varmista ohjaus- ja hallinta-aseman (GCS) asetuksista, että kamera ei tarjoa tahatonta näkyvyyttä droneasi ympäröiville alueille.
- Käytä virtuaalista yksityisverkkoa (VPN) yhteydellä, jolla jaat kuvia ja videoita.

Dronen ohjaus ja valvonta GCS:n kautta (käsiohjain, kannettava tietokone, tabletti tai älypuhelin)

Varo: Drone ja GCS kommunikoivat keskenään yleensä radiotaajuuksilla välittäessään ohjauskäskyjä tai hyötydataa (sijaintitietoja, videoita, valokuvia tai muuta dataa). Rikolliset voivat yrittää murtautua GCS:ään tai sen yhteyksiin häiritäkseen toimintaa, saadakseen dronesi hallintaan tai päästäkseen sen hyötykuorman tuottamiin tietoihin.

Huomioi:
- Varmista, että GCS-laiteohjelmisto on ajan tasalla.
- Käytä virtuaalista yksityisverkkoa (VPN) yhteydellä, jolla siirrät kuvia ja videoita tai muuta hyötydataa.

LENNON JÄLKEEN

Kun lataat, siirrät ja tallennat dronesi tietoja, varmista, että ne ovat suojattuja.

Drone-lennon tietojen tallentaminen

Varo: Drone-lennon tiedot voidaan ladata, siirtää ja tallentaa lennon päätyttyä. Yksi 30 minuutin drone-lento voi tuottaa 500 valokuvaa vaatien jopa yli 3 gigatavua tallennustilaa. Maasta riippumatta drone-yritykset voivat kerätä ja säilyttää tietoja, kuten henkilötietoja, valokuvia ja videoita; myös dronen reittitiedolla voi olla kysyntää.

Huomioi:
- Lue ohjelmistojen käyttäjäsopimukset ja tietosuoja-käytännöt ymmärtääksesi, minne tietosi siirretään, tallennetaan ja mahdollisesti jaetaan.
- Käytä fyysistä yhteyttä (lukija tai johto) hyötykuorman tuottaman datan lataamiseen jatkokäsittelyä varten.
- Poista jokaisen käytön jälkeen kaikki henkilökohtaiset tiedot dronestasi ja irrotettavista tallennusmedioista.
- Tiedosta mihin dronen käytön tiedot tallentuvat.

Lisäresurssit

- **CISA UAS verkkosivusto:** cisa.gov/unmanned-aircraft-systems
- **CISA:n Suojaa dronesi – Tietoturvaa ja -suojaa koskevat ohjeet:** https://www.cisa.gov/sites/default/files/2023-01//FINAL_508 Compliant_Secure Your Drone_Privacy and Data Protection Guidance_24JAN2023.pdf
- **CISA: n kyberturvallisuuden parhaat käytännöt kaupallisten UAS-järjestelmien käyttämiseen:** cisa.gov/publication/cybersecurity-best-practices-operating-commercial-unmanned-aircraft-systems
- **CISA: n kyberturvallisuuden suorituskykytavoitteet:** cisa.gov/cpg
- **CISA Cyber Essentials:** cisa.gov/publication/cisa-cyber-essentials
- **CISA: n monivaiheinen todennus:** cisa.gov/mfa
- **CISA raportti tietojenkalastelusta:** cisa.gov/uscert/report-phishing
- **CISA Shields Up:** cisa.gov/shields-up
- **CISA Stop Ransomware:** cisa.gov/stopransomware
- **Blue UAS hyväksyttyjen luettelo:** diu.mil/blue-uas-cleared-list
- **FAA: n ohjeet droonien turvallisesta käytöstä:** faa.gov/uas
- **UAS harrastelennättäjien turvallisuustesti:** faa.gov/uas/recreational_Lentolehtiset/knowledge_test_updates

Mitä tehdä, jos olet tietoverkkorikoksen uhri

- ☐ tee rikosilmoitus poliisille ja ilmoita tapahtumasta Kyberturvallisuuskeskukselle

Traficomin verkkosivusto sekä ilmailuun, että kyberturvallisuuteen liittyen: https://traficom.fi/fi

Liitteenä joukko tarkentavia ohjeita perustuen ohjeeseen CISA: Kyberturvallisuuden parhaat käytännöt kaupallisten UAS-järjestelmien käyttämiseen.

Tarkentavia ohjeita

Jos hyötykuorman datayhteys muodostetaan miehittämättömän ilma-alusjärjestelmän (UAS) ja tallentimen välille Wi-Fi -yhteyksien kautta, niin tee voitavasi yhteyden suojaamiseksi:

- Varmista, että datalinkki tukee salausalgoritmia Wi-Fi -tietoliikenteen suojaamiseksi.
- Käytä WPA2-AES -suojausstandardeja tai sitä turvallisimpia saatavilla olevia salausstandardeja.
- Käytä monimutkaisia salausavaimia, ja vaihda ne säännöllisesti. Varmista, että salausavaimet eivät ole helposti arvattavissa eivätkä liity miehittämättömän ilma-alusjärjestelmän merkkiin, malliin tai sen käyttöorganisaatioon.
- Käytä monimutkaisia SSID-tunnuksia (Service Set Identifier), jotka eivät liity miehittämättömien ilma-alusjärjestelmien toimintoihin. Vältä miehittämättömän ilma-alusjärjestelmän merkin, mallin tai käyttöorganisaation sisältymistä SSID tunnukseen.
- Määritä UAS olemaan lähettämättä yhteyden SSID:tä tai verkkonimeä.
- Vaihda salausavaimet turvallisessa paikassa, jotta vältät salakatselun, joko fyysisen tai kameralla tehtävän.
- Jos UAS tukee TLS (Transport Layer Security) -protokollaa, varmista, että siitä on käytössä korkein standardin versio, käytännössä TLS 1.2 tai uudempi.

Salaa UAS-ohjauksen ja telemetrian sekä hyötykuorman datayhteys (kuvat, video ja ääni tai muu hyötydata) eri avaimilla.

Varmista, että miehittämätön ilma-alusjärjestelmä pystyy salaamaan alukselle tallentuvat tiedot.

Käytä erillisiä UAS-järjestelmään liittyviä mobiililaitteita, joissa ei ole ulkoisia yhteyksiä, tai poista käytöstä kaikki yhteydet Internetin ja miehittämättömän ilma-alusjärjestelmän sekä UAS-järjestelmään liittyvien mobiililaitteiden välillä käytön aikana. Harkitse langattoman liikenteen analysaattoreiden käyttämistä lisätäksesi ymmärrystäsi UAS-viestintäliikenteestä.

Käytä mobiililaitesovelluksia virtuaalisessa kokoonpanossa (sand-box) osana laitteiden käytön turvallisuutta.

Kun liität UAS:n tai siihen liittyvän siirrettävän tallennuslaitteen tietokoneeseen:

- Käytä yhteyden muodostamiseen erillistä tietokonetta, josta ei ole samaan aikaan yhteyttä Internet- tai yritysverkkoon.
- Käytä yhteydellä asiaankuuluvasti konfiguroitua palomuuria ja varmistu laitteesi haittaohjelmien tunnistuksen kirjastojen ajantasaisuus estääksesi tietojen luvaton siirtyminen tai haittaohjelmille altistuminen.
- Tiedot olisi salattava sekä säilytyksen että siirron aikana luottamuksellisuuden ja eheyden varmistamiseksi.
- Käytössä olisi oltava todentamismekanismit sellaisia UAS:iä varten, joilla on pääsy yksityisiin tai luottamuksellisiin tietoihin. Käytä monivaiheista todennusta (MFA) aina kun mahdollista UAS-toimintoihin liittyvillä tileillä.
- Noudata tallennettujen, siirrettävien ja kaikkien arkaluonteisten tietojen tiedonhallintakäytäntöjä.
- Poista kaikki tiedot UAS:stä ja siirrettävistä tallennusvälineistä jokaisen käytön jälkeen ylikirjoittamalla tai formatoimalla.

Eri UAS-valmistajilla voi olla tarjolla "omia kovennuksia" järjestelmän datan käsittelyyn, esim. DJI käyttää nimitystä "Local Data Mode" (LDM) omastaan. Voit lukea siitä lisää seuraavista linkeistä ja harkita niiden perusteella, miten toimit.

https://dronedj.com/2020/09/28/what-is-dji-local-data-mode-heres-how-it-keeps-drone-flights-secure/
https://security.dji.com/asset/files/2020_09-FTI%20Cybersecurity-Executive%20Summary%20of%20DJI%20Assessment.pdf