**Project Fasten Your Seatbelts**

**Security Handleiding**

Klas: IN104

Groep: 4

Door: Gian van Holt en Ahish Sewgobind



Inhoudsopgave

[Inleiding 3](#_Toc408347345)

[Software 4](#_Toc408347346)

[Hardware 4](#_Toc408347347)

[SPOOFING 4](#_Toc408347348)

[SSH 4](#_Toc408347349)

[Blokkeren van het internetprotocol ICMP 5](#_Toc408347350)

[Mac-Adres 6](#_Toc408347351)

[Algemene voorwaarden 7](#_Toc408347352)

# Inleiding

De raspberries in de vliegtuigen van Corendon moet niet alleen softwarematig maar ook fysiek worden beveiligd. Dit om zo te behoeden dat het niet in verkeerde handen valt of juist misbruik van wordt gemaakt.

# Software

Doormiddel van ip tables regels en ook door de captive portal proberen we de software gedeelte zo goed mogelijk te beveiligen.

# Hardware

De raspberries moeten in een beveiligde ruimte worden opgeslagen van het vliegtuig. Toegang wordt verleent doormiddel van een sleutel. Wel moet het mogelijk zijn om er gemakkelijk bij te komen maar zonder dat dit voor een werknemer of passagier hindert. Het moet mogelijk zijn dat de beheerder en/of monteur van de technische dienst erbij kan om eventueel onderhoud te doen.

Kabels worden allemaal weggewerkt, het zal niet mogelijk zijn om kabels te zien. Dit wordt of onderaan of bovenaan in het vliegtuig vastgemaakt. De raspberries zijn verbonden met een switch, deze switch verbindt met een router, die alle inkomende en uitgaande verbindingen routeert. Ook dit is een beveiligde ruimte.

# Beveiligingsmaatregelen

Er bestaan verschillende technieken om het netwerk van binnenuit kapot te krijgen.

Daardoor worden onbekende zaken zoveel mogelijk gedropt, dit houdt in dat de router netwerkverkeer zal tegenhouden indien het er verdacht uitziet. De reden waarom is om een “man in the middle” te voorkomen.

# SSH

Mogelijk is het om een firewall op te zetten voor inkomende verbinding doormiddel van kabel, denk aan SSH. Onbekende ip adressen worden dan geblokkeerd.

Ook kan dit via “ip tables”. Een belangerijk term als het gaat om beveiligen.[[1]](#footnote-1)

# Blokkeren van ICMP

Hoe moet je een icmp blokkeren? Zodat je bij het gebruik willen maken van ping een error melding krijgt.

Met het volgende manier kan je de ping blokkeren. Bij het uitproberen krijgt je de volgende melding: “Destination port unreachable”.

Voeg de volgende ip table line toe om dit toe te passen:

**iptables -A INPUT -p icmp --icmp-type echo-request -j REJECT**

Om ping te blokkeren zonder dat je een melding krijgt moet je de volgende regel toevoegen:

**iptables -A INPUT -p icmp --icmp-type echo-request -j DROP**

**iptables -A OUTPUT -p icmp --icmp-type echo-reply -j DROP[[2]](#footnote-2)**

Dit is om te voorkomen dat netwerkapparatuur wordt “geDDoSt”.

# Mac-Adres

Het volgende script kan worden toegepast als er een mangle table is aangemaakt die “INTERNET” heet.

**iptomac=$(arp -an | grep $1 | cut -d " " -f 4)**

**sudo iptables -t mangle -I NAAM -m mac --mac-source $iptomac -j RETURN**

Je maakt een variable aan die noem je “iptomac”. Daarin vermeld een commando er iets moet worden gekopieerd wanneer een apparaat verbonden is met het Corendon netwerk.

Iets is in dit geval het Mac-adres van een apparaat. Dit wordt vervolgens bewaard in de database. Voordat dit wordt bewaard moet het worden opgeslagen en dan verplaatst.

Corendon B.V levert aan haar reizigers de mogelijkheid om tegen betaling gebruik te maken van het internet tijdens de vlucht door middel van het WiFi netwerk in het vliegtuig. Mits u beschikt over een geschikte gebruikersnaam en wachtwoord en u akkoord gaat met de volgende gebruikersvoorwaarden:

1. De bandbreedte die per sessie ter beschikking wordt gesteld is onbeperkt. U heeft dus geen limiet en er komen geen extra kosten kijken als u gebruikt maakt van het WiFi netwerk.
2. De kwaliteit en snelheid kan afhangen van een aantal verschillende factoren

waaronder atmosferische storingen en de kwaliteit van de door u gebruikte randapparatuur.

1. U zult:
   1. Niets doen dat leidt tot overlast van het personeel of voor de andere reizigers die gebruik maken van de vliegtuig of het WIFI netwerk.
   2. Niet handelen in strijd met wettelijke bepalingen en het netwerk niet gebruiken voor criminele doeleinden zoals spamberichten, virussen en/of malware te verspreiden.
   3. Geen inbreuk te maken op de beveiliging van het netwerk en/of toegang proberen te verkrijgen tot de apparatuur van het vliegtuig, personeel of andere reizigers.
   4. Het dataverkeer tussen de door u gebruikte apparatuur en de accesspoint is niet versleuteld. U bent dus uiteindelijk zelf verantwoordelijk voor de beveiliging van de apparatuur waar u gebruik van maakt
2. Corendon is niet aansprakelijk voor enige schade die u zou leiden in verband met het gebruik maken van het netwerk of van het internet. Als u het daar niet eens mee bent of als u kunt bewijzen dat de schade is aangebracht door of het WIFI net werk of het personeel kunt u een klachtbrief schrijven naar onze hoofdkantoor.

1. <http://www.hobbytronics.co.uk/raspberry-pi-ssh> [↑](#footnote-ref-1)
2. <http://crybit.com/iptables-rules-for-icmp/> [↑](#footnote-ref-2)