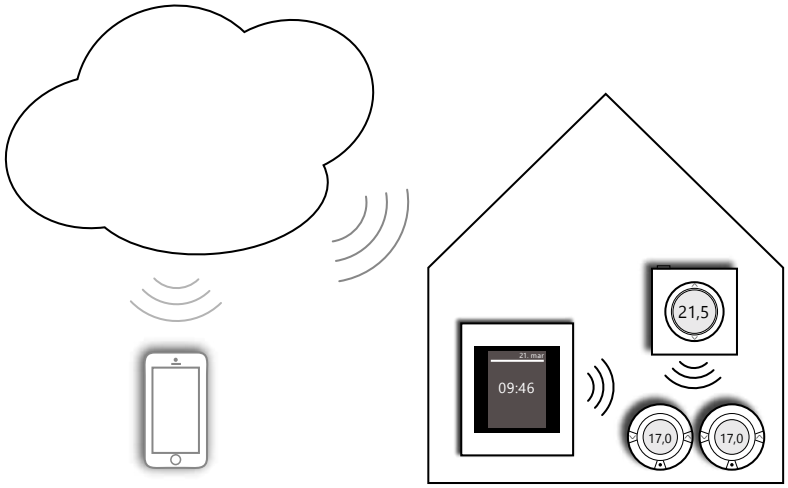
ENGINEERING TOMORROW

Teknisk dokument

Datasikkerhed for *Danfoss Link™*

Baggrund



Danfoss Link™ består af tre hoveddele:
- Z-Wave-komponenter (i huset)
- Link™ til serveren i skyen (hus til internet)
- Serveren i skyen til appen (internet)

I huset – trådløs Z-Wave:
- **Anvendelse:** Z Wave-netværk overfører trådløst temperaturer, sætpunkter og varmemeddelelser mellem termostater, rumfølere og Link™ panelet.
- **Sikkerhed:** Data overføres ved hjælp af sikre beskyttede protokoller.

Ud af huset – Link™ til serveren i skyen:
- **Anvendelse:** Kun de data, f.eks. temperatur i et rum, der anmodes om, sendes til skyen og videre til den app, der anmoder om dem.
- **Sikkerhed:** Wi-fi-forbindelse fra Link™ til routeren ved hjælp af WPA2-kryptering. Link™ til serveren i skyen krypteres også ved hjælp af AES-kryptering og er meget sikker.

Serveren i skyen til appen:
- **Anvendelse:** Sender de data, der anmodes om, til appen eller anmoder om data fra serveren i skyen.
- **Sikkerhed:** Serveren i skyen til appen krypteres også ved hjælp af AES-kryptering.

Sikkerhed

Sikkerhed mod trusler:
Serveren i skyen og Link™ beskyttes mod hacking ved hjælp af AES-kryptering. Ud over at verificere, at krypteringen virkelig giver en stærk beskyttelse, testes sikkerheden hvert år af uafhængige datasikkerheds-specialister, der forsøger at hacke sig ind i systemet*. Herudover udføres der løbende kodeefterprøvninger for at verificere, at der ikke findes nogen bagdøre.

Databeskyttelse:
Brugerdata såsom temperaturer eller sætpunkter gemmes kun i skyen, hvis du giver tilladelse til det, så databeskyttelsen sikres yderligere. Se den gyldige slutbrugerlicensaftale.

Systemintegritet:
Danfoss Link™ systemet er ikke forbundet med systemer, der ikke kommer fra Danfoss, og svækkes derfor ikke af andre systemer.

Fysisk beskyttelse:
En pinkodefunktion sikrer, at kun administratoren kan betjene Link™.

Der udføres flere test for at hacke ind i *Danfoss Link*™ systemet, herunder men ikke begrænset til:
- Denial of Service-angreb (DOS)
- Indskydelse + portscanning
- Manglende adgangskontrol til funktionsniveau
- Fejlkonfiguration af sikkerhed
- Eksponering af følsomme data

**Advanced Encryption Standard eller AES er en symmetrisk blokkryptering, der bruges af den amerikanske regering til at beskytte hemmeligstemplede oplysninger, og den er implementeret i software og hardware verden over for at kryptere følsomme data. Kilde: Techtarget*

Kommunikation

Sikring af det højest mulige datasikkerhedsniveau.

- Data i skyen beskyttes ved hjælp af den krypteringsstandard, der bruges af den amerikanske regering til at beskytte hemmeligstemplede oplysninger.
- Systemet testes årligt af uafhængige datasikkerhedsspecialister.
- En pinkodefunktion sikrer, at kun administratoren kan betjene Link™.
- Brugerdata såsom temperaturer eller sætpunkter gemmes kun i skyen, hvis du giver tilladelse til det. Se den gyldige slutbrugerlicensaftale.

Danfoss A/S
Heating Segment, Salg Danmark • varme.danfoss.dk • +45 6991 8080 • E-Mail: kundeservice.dk@danfoss.com