AFGØRELSE FRA TELEANKENÆVNET

Sag: 23-19

KLAGENS INDHOLD OG FORLØB

Klager havde i en længere årrække en internetforbindelse via kabel-tv-antennestikket (coax) hos indklagede. Indklagede stillede en router til rådighed for klager til brug for forbindelsen.

Den 19. december 2022 sendte klager en skriftlig klage til indklagede. Klager var blevet hacket af naboens søn og ønskede sikkerhed for, at det kun var muligt for relevante personer at ændre i routerens opsætning. Klager henviste til, at det var et problem, at routeren kunne styres via WiFi.

Indklagede svarede på mail samme dag og henviste klager til at kontakte indklagedes hotline. Indklagede oplyste også, at klagers forbindelse var blevet fejlmeldt, og at en tekniker ville kontakte klager telefonisk den 3. januar 2023.

Den 29. december 2022 sendte klager en ny mail til indklagede med yderligere oplysninger og spørgsmål vedrørende routeren.

Den 3. januar 2023 havde klager og en medarbejder hos indklagede en telefonisk samtale om klagers spørgsmål og ønsker til routeren.

Efterfølgende sendte indklagede en mail den 3. januar 2023 og oplyste, at det ikke var muligt at imødekomme et ønske om spærring af Wi-Fi GUI (Graphical User Interface). Indklagede henviste klager til at melde hacking til politiet.

Klager indbragte herefter sagen for Teleankenævnet.

Sagen har i forbindelse med nævnsbehandlingen været forelagt en teknisk sagkyndig.

PARTERNES KRAV OG BEGRUNDELSER:

Klager

Klagers krav til indklagede er, at indklagede ændrer firmware på klagers router, så det ikke er muligt at få adgang til lokaladministration eller sitet MitWifi.dk fra en Wi-Fi forbindelse, men kun via et tilsluttet kabel.

Når sikkerheden senere hen måtte være forbedret i forhold til, hvem der kan foretage ændringer, kan det ændres til normal standard.

Klager har fremsat forslag til indklagede om at knytte login og ændringer via MitWifi.dk sammen med f.eks. 2 faktor funktion eller NemID/MitID.

Klager har oplyst, at udviklingen i, hvordan man hacker et Wi-Fi password, accelerer pga. moderne værktøjer, så det ikke tager mange minutter at hacke sig ind på et fremmed Wi-Fi netværk. Det kan nu gøres vha. en App på en mobiltelefon, så selv forbipasserende ude på gaden kan hacke sig ind på et fremmed Wi-Fi netværk. Det er klagers opfattelse, at et password på 10 tegn ikke længere er nogen sikkerhed for, at man er beskyttet. Klager har henvist til, at der findes et utal af videoer på f.eks. Youtube, som viser hvordan passwords nemt kan hackes.

Naboens søn, som hackede klagers router, har aldrig været inde hos klager, og routeren er gemt bag Tv'et, så man kan ikke aflæse passwordet uden videre.

I forhold til indklagedes router er det muligt at administrere denne fra WiFi. Har en udenforstående først skaffet sig adgang til Yousee hjemmenetværket, så kan vedkommende uden de større problemer tage fuld kontrol over Wi-Fi netværket ved at kalde sitet MitWifi.dk (et site, som er knyttet til indklagede, og som er lavet med det formål, at det er nemt at administrere passwords mv for den husstandsrouter, man har i sit abonnement). Men der er intet, der sikrer, at det er abonnenten eller en fra dennes husstand, som laver ændringerne på husstandsrouteren.

Som en midlertidig løsning havde klager bedt om, at man på klagers router kunne slå lokal administration fra via Wi-Fi, så det kun var muligt at få adgang til lokaladministrationen af routeren via et kabel. Dette blev afslået med den begrundelse, at det måtte man som princip ikke gøre.

Klager har anført, at dette ikke er en sag for politiet, da klager står uden nogen form for bevis for, hvilken mobiltelefon der er anvendt til at skaffe adgang til routeren og klagers netværk.

Klager understreger, at det er bekymrende, at indklagede ikke tager højde for dem, der forsøger at bryde ind i deres kunders netværk. En lille sårbarhed i WiFi-hjemmenetværket kan give en kriminel adgang til næsten alle de enheder, der opretter forbindelse til det pågældende netværk. Hackere og svindlere kan muligvis få adgang til kundens online bankkonti eller kreditkortportaler. De kan endvidere muligvis læse de e-mails, man sender til sin læge. De kan endda oversvømme ens enheder med Malware og spyware.

Det er på denne baggrund klagers opfattelse, at indklagede bør sikre sine routere bedre.

Indklagede

Indklagede afviser klagers krav og fastholder, at indklagede leverer en sikker router.

Vedrørende sikkerhed på Wi-Fi har indklagede oplyst, at det er vigtigt at sikre routerens Wi-Fi med et godt password. Indklagede anbefaler også, at kunderne ændrer deres passwords både til Wi-Fi og til routerens brugerinterface (GUI).

Default password til routerens GUI (Admin password) er på 8 karakterer, og Wi-Fi Adgangskoden er på 10 karakterer. De er noteret på en label på routeren. De 2 default passwords er komplekse, og det vil ikke være muligt at bryde dem på få minutter via en app.

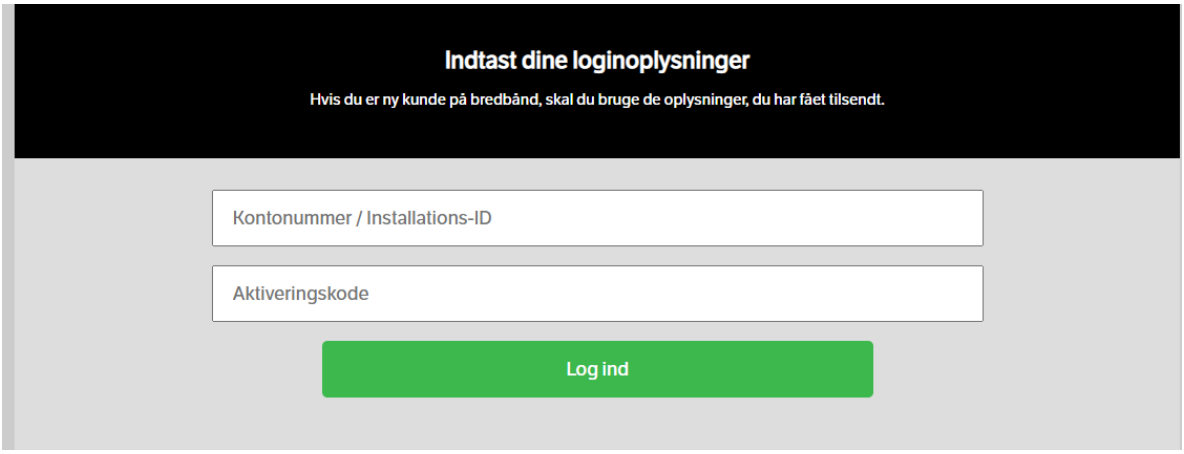
Indklagede anbefaler dog at ændre de 2 passwords, da det vil være muligt at aflæse dem på routeren, hvis man er i nærheden af routeren, og i så fald vil kompleksiteten af de 2 forudbestemte passwords ikke give den nødvendige beskyttelse.

Indklagede har oplyst, at der er 2 måder at administrere ens netværk på nemlig via hjemmesiden mitwifi.dk og via routerens brugerinterface (GUI).

Fra hjemmesiden https://mitwifi.dk har man som standard mulighed for at administrere sit Wi-Fi setup. Når siden tilgås, vil resultatet kunne udmønte sig på 2 måder.

Såfremt siden tilgås fra en enhed, der er tilsluttet ens eget hjemmenetværk, vil der ikke skulle anvendes login til siden. Der vil ikke være forskel på, om det sker fra en kablet enhed eller en enhed, der er tilsluttet via Wi-Fi.

Såfremt siden tilgås fra en enhed, som ikke er tilsluttet ens eget hjemmenetværk, vil man blive præsenteret for en side, som kan ses på nedenstående skærmdump.



Her skal man, før man kan administrere sin Wi-Fi, indtaste oplysninger, som kunden har fået i forbindelse med installationen af bredbåndsforbindelsen.

Kontonummer/Installations-ID fremgår på bekræftelsen for oprettelsen eller efterfølgende ændring af abonnementet samt på regningerne. Aktiveringskoden bliver ved oprettelsen af internetforbindelsen tilsendt pr. mail eller sms.

Hvis man som kunde slet ikke ønsker muligheden for at kunne administrere sit Wi-Fi via https://mitwifi.dk, er det muligt at kontakte YouSee og anmode om at få administrationsadgangen fjernet. I så fald vil administrationen af ens Wi-Fi skulle ske via routerens GUI.

Det er sikret at man kun kan tilgå routerens brugerinterface via ens eget hjemmenetværk. Routerens brugerinterface kan tilgås ved at taste http://192.168.0.1. Dette fremgår også af en label på routeren. Der vil ikke være forskel på, om det sker fra en kablet enhed eller en enhed, der er tilsluttet via Wi-Fi.

Det er ikke muligt at begrænse adgangen til mitwifi.dk eller routerens brugerinterface til kun at kunne lade sig gøre via en kablet forbindelse og dermed udelukke adgangen via Wi-Fi. Det er endvidere ikke muligt at indføre 2 faktor godkendelse eller login validering med-MitID.

Indklagede vurderer løbende sikkerheden, da teknologien udvikler sig eksponentielt. Derfor øger indklagede også minimumskravet til passwords til 14 karakterer fremadrettet, og indklagede vil selvfølgelig løbende revurdere dette.

Når man har fysisk adgang til udstyret, kan man til hver en tid nulstille udstyret ved mistanke om misbrug. Derved kan man smide eventuelle uvedkommende af, og lave et nyt sikkert password, hvorefter man har fuld kontrol over sit netværk.

NÆVNETS BEMÆRKNINGER

Nævnet bemærker indledningsvist, at der mellem parterne er enighed om, at indklagede leverer en internetforbindelse via coax til klager og har gjort det gennem længere tid. Nævnet lægger efter det oplyste til grund, at indklagede til brug for internetforbindelsen har stillet en router til rådighed for klager af mærket Sagemcom model F@ST 3890v3.

Klager gør over for ankenævnet gældende, at den af indklagede leverede router ikke er sikker, og at der derved er let adgang for uvedkommende til at hacke sig ind på klagers netværk. Indklagedes levering har derfor været mangelfuld, hvorfor klager gør gældende, at indklagede skal udbedre dette ved at ændre indstillingerne i routeren.

Indklagede afviser, at routeren er mangelfuld. Indklagede henviser til, at det er vigtigt med et sikkert og komplekst password. Indklagede har ligeledes henvist til, at når man har fysisk adgang til udstyret, kan man til enhver tid nulstille dette og derved smide evt. uvedkommende personer af. Indklagede har også anført, at det er sikret, at man kun kan tilgå routerens brugerinterface via ens eget hjemmenetværk.

Nævnet bemærker, at det som udgangspunkt er klager, der skal godtgøre, at indklagedes ydelse har lidt af mangler, og at disse mangler har været så væsentlige, at klager kan kræve udbedring i form af ændret opsætning og mulighed for at tilgå netværket for at foretage ændringer i routerens indstillinger.

Sagen har været forelagt en teknisk sagkyndig.

Nævnet noterer, at den teknisk sagkyndige har udtalt, at der som sådan ikke er forskel på sikkerheden i forhold til de forskellige typer/modeller af routere. Den teknisk sagkyndige har derimod udtalt, at længden af et password ofte bruges som udtryk for graden af sikkerhed. Den sagkyndige har videre udtalt, at når et password hackes, er det sjældent, fordi koden brydes, men fordi brugerne af nettet har håndteret password på en usikker måde. Det er den sagkyndiges vurdering, at den anvendte router er en meget populær model, som bruges i hele verden.

I forhold til, om det er let at hacke sig ind på et hjemmenetværk, har den teknisk sagkyndige anført følgende: *"Et hjemmenet der bruger WiFi er som udgangspunkt altid nemt at komme ind på som hacker (hvis man gerne vil). Der findes et hav af muligheder – og er man tålmodig vil der altid «over tid» findes en løsning."*

Nævnet noterer videre den sagkyndiges svar omkring blokering af GUI via WiFi, hvorefter dette næppe vil være muligt, da det skal implementeres af producenten. Det er den sagkyndiges vurdering, at det heller ikke vil give meget mere sikkerhed, men måske skabe lidt mere besvær.

Nævnet bemærker, at klager på baggrund af den teknisk sagkyndige udtalelse har fremsat yderligere bemærkninger. Klager har blandt andet peget på en række sikkerhedsmangler, som ifølge klager kan imødegås eller minimeres ved de af klager foreslåede foranstaltninger.

Nævnet finder på baggrund af ovenstående og sagens omstændigheder i øvrigt ikke at det er godtgjort, at der har været så væsentlige mangler ved routeren, at klager kan kræve udbedring af indklagede. Nævnet finder på baggrund af den tekniske sagkyndige vurdering heller ikke grundlag for at fastslå, at routeren eller indklagedes brug og opsætning heraf kan anses som værende mangelfuld.

Nævnet finder desuden ikke, at indklagede kan pålægges at anvende 2 faktor login til siden mitwifi.dk.

Klager gives af ovennævnte grunde ikke medhold i klagen.

Nævnet træffer herefter følgende:

AFGØRELSE

Der gives ikke klager, NN, medhold i klagen over indklagede, Yousee A/S.

Det indbetalte klagegebyr på 175 kr. returneres ikke til klager, jf. vedtægternes § 27.

Indklagede, Yousee A/S, bidrager som tilsluttet Teleankenævnet til nævnets drift og betaler derfor ikke sagsomkostninger, jf. vedtægternes § 28.

På Teleankenævnets vegne, den 21. marts 2024.