

Du kan bli utsatt for hacking når du bruker et åpent, usikret trådløst nettverk fordi data potensielt sendes i klartekst i et ukryptert nettverk.

Faren i trådløse nett



Simon Mangelrød,
Technical Manager Intility
Operations Center

Mange er kanskje ikke klar over at det kan innebære en betydelig sikkerhetsrisiko å surfe på trådløse nett (WiFi). Nedenfor følger noen tips som kan gjøre det sikrere å surfe på trådløse nett.

De fleste av oss har med mobile enheter på farten, enten det er smart-telefon, PC eller nettbrett. Gratis trådløst nettverk er tilgjengelig nærmest overalt, og kobles ofte til på offentlige steder slik som kafeer og flyplasser, men også på arbeidsplasser og på besøk hjemme hos andre.

Reell sikkerhetsrisiko

Sjansen for at du skal bli utsatt for hacking når du bruker et åpent, usikret trådløst nettverk er reell, fordi data potensielt sendes i klartekst i et ukryptert nettverk. Det betyr at passord, kredittkortinformasjon, PIN-koder og sensitive bedriftsdata enkelt kan snappes opp av noen med litt IT-kunnskap.

Flertallet benytter mobile enheter også til jobberelatert arbeid, både via e-post og dokumenter, hvilket gjør det enda viktigere å ta forholdsregler for å forhindre at data kommer på avveie. Det er ille nok om ens egne data kommer på avveie, verre er det om man selv er opphav til sikkerhetshull på egen arbeidsplass. Du slipper ikke fremmede inn på bedriftens nettverk, og som arbeidstakere må vi derfor tenke på dette når vi er på trådløse nettverk.

Sårbarhet i WiFi-protokollen WPA2

I oktober ble det avdekket en sikkerhetsbrist i krypteringsprotokollen WPA2 (WiFi Protected Access), sikkerhetsstandarden som har til hensikt å sørge for at man kobler seg sikkert til trådløse nettverk. Sårbarheten åpner opp for tyvlytting og modifisering av trafikk mellom aksesspunkt (ruter) og enheten, og kan ramme de fleste enheter som kan kobles til trådløse nettverk.

En angriper som er i fysisk nærhet av offeret, kan utnytte WPA2-sårbarheten til å få tilgang til informasjon som vanligvis er beskyttet av krypteringen mellom enheten og senderen. Siden dette er en sårbarhet i WiFi-standarden, er den ikke begrenset til spesifikke implementasjoner eller produkter. Dette betyr at hackere kan angripe alle plattformer, og all informasjon som sendes ukryptert over WPA2-nettverk kan i utgangspunktet leses.

Avhengig av nettverkskonfigurasjonen er det også mulig for en angriper å manipulere data eller installere skadevare inn i offerets nettrafikk. Spesielt trafikk som går til ukrypterte sider (HTTP) er sårbare. Siden sårbarheten

gjelder enheter i et trådløst nettverk, og ikke selve aksesspunktet, vil ikke angriper få tilgang til passordet på det trådløse nettverket, selv om angrepet er vellykket. Det er derfor ikke nødvendig å bytte passord på den trådløse ruter eller på trådløst nettverk.

Generelle sikkerhetstips for trådløse nettverk

• Oppdater programvare og operativsystem på alle enheter

Sørg for at du oppdaterer programmer så snart du får melding om at oppdateringer er tilgjengelige, slik at du er sikker på at dine programmer ikke har sikkerhetshull. Dette gjelder også for mobil og nettbrett.

• Benytt sikrede trådløse soner fremfor usikrede

Hvis du skal benytte et trådløst nett, hold deg til sikrede trådløse soner. Disse kjennetegnes ved at de krever passord eller ved at man må logge på en portal for å få bruke nettet.

• Unngå trådløse soner med ukjente navn

Kafeer, hoteller og andre steder som tilbyr trådløse soner, har gjerne firmanavnet sitt i sonenavnet. Unngå soner hvor du ikke vet hvem som eier nettverket (f.eks. «Gratis

internett»). NB: Det er heller ingen garanti for at «Firma X» faktisk tilhører dette firmaet.

- **Påse at trafikken er beskyttet med HTTPS**

Sjekk at du benytter «sikre» nettsider.

- **Bruk VPN eller Citrix hvis mulig**

Så sant det er mulig, bør du benytte VPN eller Citrix om du skal jobbe med bedriftsrelaterte saker og dokumenter. Med VPN eller Citrix krypteres datatrafikken, slik at du er sikker på at dataene ikke kan snappes opp og misbrukes.

- **Kjøp enheter av leverandører som tar sikkerhet på alvor**

Det er store avvik mellom leverandører når det gjelder i hvilken grad de tar sikkerhet på alvor og om de faktisk lager oppdateringer til produkter som er ute på markedet.

Apple, Google og Microsoft, som de største leverandørene av operativsystem, tar alle sikkerhet svært alvorlig. Når det gjelder Android-enheter (der operativsystemet er laget av Google), er man helt avhengig av om produsenter som for eksempel Samsung/Sony/LG/Huawei, sender ut oppdateringer.

Mobildata sikrest

Sårbarheten i WiFi-protokollen WPA2 understreker at også såkalt sikre trådløse nettverk kan utgjøre en sikkerhetsrisiko, og at tipsene ovenfor dermed ikke kan garantere sikker surfing. Det trådløse nettet bør derfor skrus av hvis det ikke brukes. For å minimere sikkerhetsrisikoen når du surfer i offentlige rom, bør du benytte mobildata, for eksempel 3G eller 4G, og dermed unngå å benytte trådløse nettverk. Stadig flere teleoperatører har store mengder inkludert mobildata og surfing på nettet i utlandet uten ekstra kostnad.