



## Slik bygger du et sikkert trådløst nettverk



Er du en av de som fremdeles er skeptisk til sikkerheten i trådløse nettverk? Det er kanskje på tide å bli kvitt gamle fordommer og gå videre. Med dagens teknologi er nemlig et sikkert trådløst nettverk fullt ut mulig, men – it-avdelingen må gjøre leksene sine først.

### → SEIGLIVDE MYTER

Det finnes fortsatt myter om hvor usikre trådløse nettverk er, med påfølgende risiko for datainnbrudd, ubudne gjester på serveren, identitetstyverier og manipulasjon av kundedata. Trass i en rivende utvikling og økt fokus på sikkerhet i den tekniske verden, preger fordommene fortsatt mange av vurderingene som blir gjort.

### UTFORDRINGENE ER HÅNDBERBARE

Ny teknologi som utfordrer sikkerheten er som vanlig på full fart fremover. Den stadige dragkampen mellom sikkerhetsbransjen og de som utfordrer den vil alltid finnes. For brukere flest er løsningen å alltid ha mest mulig oppdatert teknologi. En gammel kryptering som WEP bruker man eksempelvis kun et par minutter på å knekke med informasjon og verktøy som finnes enkelt tilgjengelig. Når det er sagt får også den nyeste sikkerhetsteknologien for trådløse nettverk bryne seg på ny teknologi og stadig mer sofistikerte angrepsmetoder.

### MULIGHETENE – LØNNSOM MOBILITET

Ved innføring av nye systemer og rutiner vil som vanlig alle avgjørelser være preget av kostnader. Snur man derimot fokuset og ser lønnsomheten i bedre mobilitet, vil man raskt se inntjeningspotensialet i trådløse nettverk. Dette kan være noe så simpelt å kunne tilby eksterne en forbindelse mot eget bedriftsnett under et besøk. Med rett teknologi kan dette gjøres enkelt og uten risiko både for tilbyder og den besøkende.

Også internt viser regnestykker at man raskt kan tjene inn kostnadene med å sette opp trådløst nettverk. Kommer man tidlig til et møte kan man bruke fem minutter på å oppdatere seg på e-post uten å måtte finne et tilkoblingspunkt. På reiser har man hele tiden sikker tilgang til bedriftens interne dokumenter. Selv moderate kalkyler viser at en mellomstor bedrift hurtig vil spare inn kostnadene til investering.

---

– Selv moderate kalkyler viser at investeringen i et sikkert trådløst nettverk raskt lar seg tjene inn.

---

### HVA SÅ MED SIKKERHETEN?

Sikkerheten i trådløse nettverk består ofte av tre hovedfaktorer: autentisering, konfidensialitet og integritet. Man skal være sikker på hvem man mottar data fra, vite at ingen utenforstående kan tyde den og at ingen har endret på innholdet. For bedrifter anbefales en sentralisert autentiseringstjener. På denne måten vil alle i nettverket få egne, unike passord. En av fordelene med dette er at da trenger man ikke informere samtlige om et nytt passord hver gang noen slutter eller et passord blir lekket.

Når man vet hvem man kommuniserer med er det tid for selve dataoverføringen. Innenfor eget trådløst nettverk vil oppdaterte krypteringsalgoritmer sikre både kon-

fidensialitet og integritet. Er den ansatte derimot i et ukjent eller eksternt nettverk, bør man sikre seg på andre måter. Virtuelle private nettverk (VPN) skaper en sikker tunell mellom den ansatte og bedriftens sikre nettverk. Med denne kombinasjonen kan man kommunisere sikkert uavhengig av hvor man befinner seg.

## DET SVAKESTE LEDD

I en helhetlig løsning der risikoene er belyst vil man kunne nyte godt av mobilitet under sikre forhold. En helhetlig løsning er derimot ikke utelukkende løst ved tekniske nyvinninger. Brukeren er som regel det svakeste ledd sett i et sikkerhetsperspektiv.

Gule lapper med passord, uforsiktighet ved inntasting av passord og enkle passord som eget navn og fødselsdato er alle med på å gjøre nettverket mer usikkert. For at man skal ivareta sikkerheten er bedriften også avhengig av en gjennomtenkt sikkerhetspolicy. Denne bør både dekke hvordan brukere oppfører seg i det trådløse miljøet, og hvordan tilgjengelighet av utstyret som tilbyr tilgangen skal være. En gjennomført total-løsning vil gjøre et trådløst nettverk like sikkert som et kablet.

## SLIK INNFØRER DU SIKKERT WLAN

Listen nedenfor kan være en nyttig huskelapp for it-sjefen med ansvar for innføring av trådløst nettverk:

### – En gjennomført total-løsning vil gjøre det trådløse nettverket like sikkert som et kablet.

#### 1. Sikkerhetspolicy

Oppdater bedriftens sikkerhetspolicy. En manglet eller svak sikkerhetspolicy skaper usikkerhet i organisasjonen og kan føre til sikkerhetshull med risiko for kompromittering og tap av data.

Typiske sikkerhetsrisikoer vil være:

- Uautorisert tilkobling til virksomhetens nettverk
- Uautorisert tilgang til virksomhetens data
- Brudd på konfidensialitet og integritet

Mye kan løses med enkle kjøreregler for alle brukere og for dem som administrerer systemet. Noen eksempler:

- Sett ikke opp andre aksesspunkt i LANet
- Ikke bruk både kablet og trådløst nettverk samtidig.
- Brukere som kobler seg opp mot andre nettverk.
- Fra eksterne lokasjoner må en bruke VPN og gå på internett via bedriftens brannmur



**Trådløse nettverk er en viktig del av ethvert fremtidsscenario og danner grunnlaget for veldig mye av den nye teknologien som vil komme i årene fremover. Den gamle kablet er trygg og god, men gir kanskje ikke så mange nye muligheter?**

#### 2. Utføre en «site survey»

Site Survey eller radioplanlegging er en fysisk gjennomgang av arealene som skal dekkes av det trådløse nettverket med måling av signalene. Denne gjennomgangen må utføres før utstyret rulles ut.

Radioplanleggingen bør skje med bruk av spesielle verktøy og ditto kunnskap. Den bør ende opp med et oversiktskart med korrekt plassering av radio og dekningsområde per radio, signalstyrker, valg av antenner og en kanalmatrise med plan for optimalt kanalvalg. Målingen bør skje fysisk på stedet og i arbeidstid, siden også mennesker absorberer trådløse signaler.

#### 3. Innfør nødvendige sikkerhetstiltak

- Soneinndeling: Bruk av VLAN (Virtuelle LAN) med oppspalting i mindre virtuelle nettenheter med definerte rettigheter.
- Aktivere kryptering: Den tidligere brukte WEP-krypteringen holder ikke mål, og WPA-krypteringen begynner også å bli avleggs. WPA2 anbefales, ikke minst på grunn av autentiseringsmulighetene.
- Deaktivere SSID-broadcast: Funksjonen som kringkaster navnet på nettet kan skrur av, slik at bare de som kjenner navnet på nettverket kan kople seg på.
- Filtrere etter MAC-adressene: Hver maskin har sitt unike navn, og bare de som er godkjent kan kople seg på.
- Innføre digitale sertifikater: Den enkelte bruker har digitale autentiseringspapirer som bare han eller hun har tilgang til.
- Fysisk sikring av aksesspunktene: Det hjelper ikke med all mulig sikkerhet hvis et aksesspunkt er tilgjengelig for uvedkommende.
- Sentral styring og administrasjon: Sikrer oversikt over brukere, tilgangsnøkler, den enkeltes rettigheter og hvem som kan styre det hele.
- Fjernaksess med VPN: En tunnel mellom klient og arbeidssted hindrer utenforstående i å gå inn på linjen når brukeren er tilkopledd arbeidsstedet. Brukeren kan da benytte arbeidsstedets brannmur og beskyttelse fra eksterne lokasjoner.
- Nettverksovervåking: Systemer lagd for å oppdage uvanlig bruk av nettverket vil

### – Oppdater sikkerhetspolicyen og spre ordet. Ikke overraskende er det brukerne som er bedriftens sikkerhetstrussel nr. 1.

kunne oppdage unaturlig oppførsel i nettverket.

- Logisk sikring av hver klient/PC: Alle tilknyttede maskiner må ha et sikkerhetsnivå tilsvarende det som er definert i virksomhetens policy.
- Skru ned sendeeffekten: Man trenger kun nødvendig effekt for å betjene maskinene innenfor en definert sone, men ikke så mye at det dekker hele nabolaget. Man kan i tillegg dekke vegger med materialer som stopper trådløse signaler.

Kontakt



Solveig Skumlien Nilsen  
avdelingsleder  
e-post: [ssn@steria.no](mailto:ssn@steria.no) / Tlf: 995 52 797

Steria AS  
Biskop Gunnerus' gate 14A  
Postboks 2, N-0051 OSLO

➔ Gå inn på [www.steria.no/guide](http://www.steria.no/guide) og få tilgang til et helt bibliotek med gratis 3-minutters guider.