Sikkerhed i trådløse netværk

IT- og Telestyrelsen
Ministeriet for Videnskab
Teknologi og Udvikling

IT- og Telestyrelsen
Holsteinsgade 63
2100 Kbh. Ø

Telefon 3545 0000
Telefax 3545 0010
E-post: itst@itst.dk
www.itst.dk

Rådet for it-sikkerhed
www.raadetforitsikkerhed.dk

Beskyt dit trådløse netværk

Der findes ingen netværk, der er 100% sikre. Du kan dog foretage en række tiltag for at sikre dit netværk. Jo bedre du sikrer dit netværk, jo dyrere og mere tidskrævende bliver det for uvedkommende at skaffe sig adgang. Du opnår altså, at det slet ikke kan betale sig for uvedkommende at skaffe sig adgang.
Ved at følge rådene i denne vejledning er det således muligt at opnå et rimeligt sikkerhedsniveau i dit trådløse netværk.

Hvorfor skal jeg særligt beskytte mit trådløse netværk?

Når netværket bruger radiobølger i stedet for kabler, betyder det, at uvedkommende nemmere kan få adgang til dine informationer

Et trådløst netværk - også kaldet WLAN - er et datanetværk, der bruger radiobølger til at sende og modtage data, hvor traditionelle datanetværk bruger kabler. Et trådløst netværk er derfor smart at bruge til bærbare computere, som ofte skal have adgang til netværket fra forskellige steder. Men det kan også være praktisk i forbindelse med at undgå at skulle trække datakabler til faste pc'er.

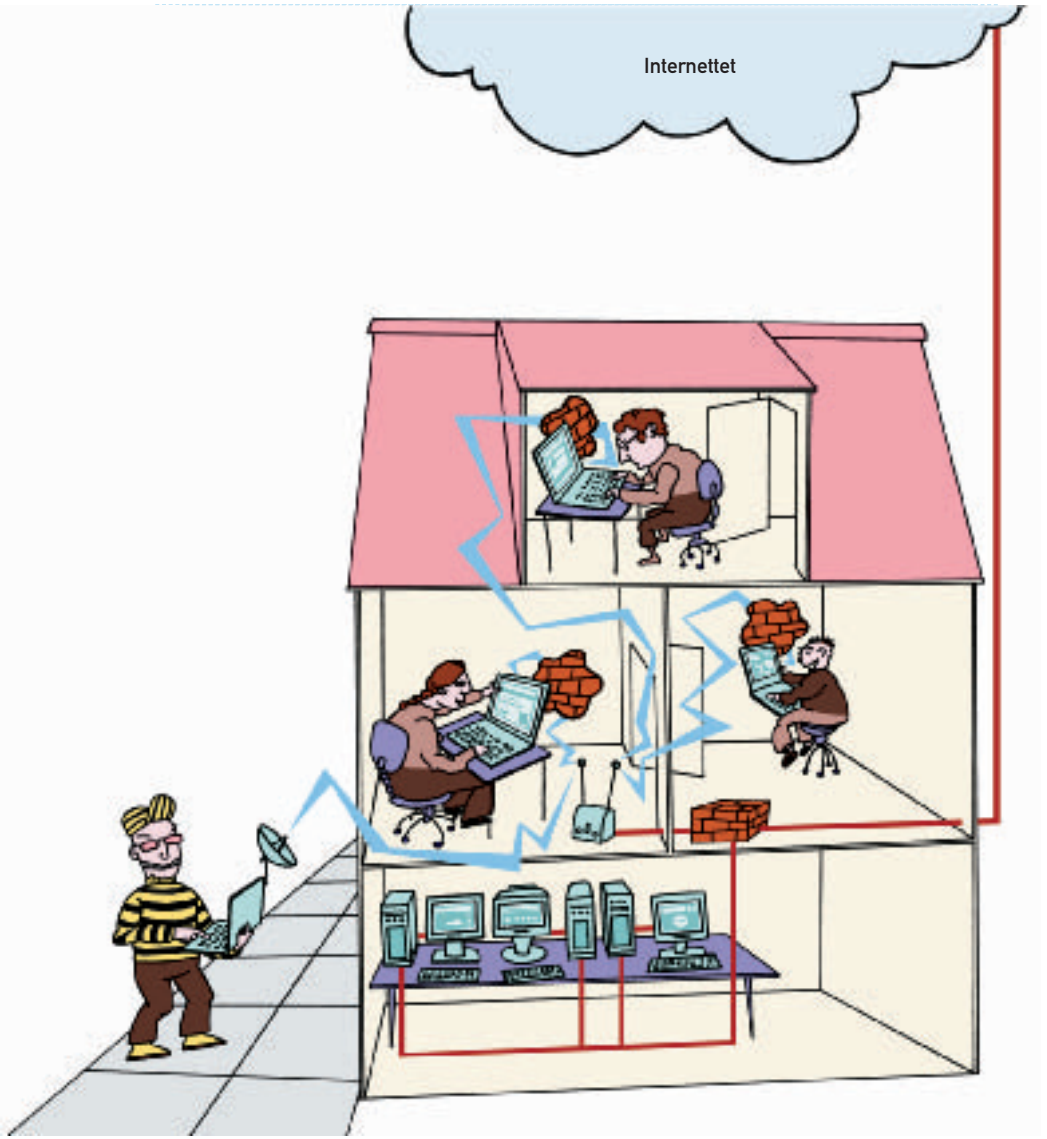
<

Radiobølgerne fra et trådløst netværk i en bygning stopper imidlertid ikke ved bygningens mure, men fortsætter udenfor. Enhver, der befinder sig udenfor, kan derfor med ganske enkelt udstyr som en bærbar pc og en antenne modtage radiobølger fra dit trådløse netværk.

Med et særligt program, som kan hentes på internettet, kan uvedkommende både se dine data og evt. ændre eller stjæle dem.

Radiobølger kan aflyttes

Et trådløst netværk uden beskyttelse er meget usikkert. Uvedkommende kan uden videre aflytte og bruge dit trådløse netværk og ændre i din computer og dit trådløse netværk. De kan også bruge din computer til at foretage angreb på andre computere. Disse angreb vil kunne spores tilbage til dig!


Internettet

Lås dørene til dit trådløse netværk

Hvordan kan jeg beskytte mit trådløse netværk?

For at modvirke at uvedkommende personer følger med i din kommunikation eller på andre måder misbruger dit trådløse netværk, er der en række forholdsregler, som du bør tage for at sikre dit trådløse netværk.

Brug kryptering

Ved anvendelse af kryptering sikrer du, at uvedkommende ikke kan få adgang til dit netværk samt at de ikke kan læse din kommunikation. Når du køber et trådløst netværk, følger der normalt en kryptering med, som hedder WPA eller WPA2. Du skal selv aktivere WPA/WPA2 på din basisstation, og du bør altid sørge for at angive et langt password (minimum 8 tegn).

Ved køb af en ny trådløs basisstation, er det vigtigt, at du sikrer dig, at den som minimum understøtter WPA og allerhelst WPA2.

Har du en gammel basisstation, er det måske ikke muligt at anvende WPA eller WPA2. Du kan dog ofte hente en opdatering til din basisstation på producentens hjemmeside, som giver mulighed for at bruge WPA eller WPA2. Hvis det ikke er muligt, bør du i stedet for bruge WEP-kryptering. WEP-krypteringen er dog mindre sikker end WPA/-

<

WPA2, og derfor er det mest sikkert at skifte WEP-passwordet tit.

Slå broadcastmeddelelser fra i dit trådløse netværk - hvis det er muligt

En basisstation udsender altid såkaldte broadcastmeddelelser, som indeholder oplysninger om navnet på dit trådløse netværk (også kaldet SSID), datahastigheden i dit trådløse netværk, og om udvekslede data er krypterede eller ej.

Man kan finde et trådløst netværk ved at lede efter disse broadcastmeddelelser. Hvis disse oplysninger opsnappes, kan hackere derefter nemt og hurtigt koble sig på det trådløse netværk.

Det er for det meste muligt at slå broadcastmeddelelser fra i et trådløst netværk. Derved gør du det sværere for hackere at finde og tilslutte sig dit netværk. Du og eventuelle andre brugere af dit trådløse netværk skal så selv taste SSID ind i de pc'er, der skal have adgang til netværket.

Husk også at ændre SSID - se næste side.

<

Husk at ændre standard password

Når du køber din trådløse basisstation fra forhandleren, er den forsynet med et standard password. Men hackerne kender de mest alminde-lige standard passwords, og har du ikke ændret standard passwordet, har en hacker meget let ved at få adgang til din basisstation og dermed foretage ændringer i opsætningen. Derfor bør du ændre standard passwordet og i øvrigt skifte det ofte.

Husk at ændre SSID

SSID er navnet på dit trådløse netværk. Hvis en ny bruger vil kobles på et trådløst netværk, skal han/hun bruge dets SSID for at få adgang. Leverandøren af din trådløse basisstation har givet den et standard SSID. Hackere kender alle standard SSID'er, så hvis du ikke ændrer dit SSID, kan de let gætte sig til navnet og få adgang til dit netværk. Du skal derfor vælge et SSID, der ikke er for nemt at gætte. Det bør for eksempel ikke indeholde informationer som dit navn eller adresse.

<

Benyt en firewall på de enkelte computere

En firewall er et program eller en hardwareenhed, der filtrerer og overvåger datastrømmen mellem flere netværk eller mellem en computer og et netværk. Internettet er usikkert, og derfor bør forbindelsen til internettet filtreres med en firewall.

Et trådløst netværk er mindst lige så usikkert som internettet. Det anbefales derfor, at alle pc'er med adgang til det trådløse netværk beskyttes med en personlig firewall. Hvis du både har trådløst og kablet netværk, bør disse også adskilles med en firewall. Se tegning på side 5.

<

Hvilken sikkerhed, du bør vælge, afhænger af værdien af de data, som du vil beskytte.

Hvad med persondata og trådløse netværk?

Hvis du håndterer personfølsomme data i dit trådløse netværk til erhvervsmæssig brug eller tænker på at gøre det i fremtiden, er der en række krav, du skal opfylde.

Disse krav er beskrevet i Persondataloven, som administreres af Datatilsynet (www.datatilsynet.dk).

Brug MAC-adresse filtrering

Alle trådløse netkort i computere har et unikt identifikationsnummer, som kaldes en MAC-adresse. Du kan derfor afskære uvedkommende fra at få adgang til dit netværk ved kun at tillade specifikke angivne MAC-adresser adgang til netværket. Du angiver de specifikke MAC-adresser, når du opsætter din basisstation.

Sikkerheden i offentlige og fælles trådløse netværk

Hvad med sikkerheden i fælles trådløse netværk eller trådløse netværk på offentlige steder?

Mange boligforeninger har valgt at deles om et trådløst netværk, og du kan også finde trådløse netværk på offentlige steder ('hot spots'). Hot spots findes f.eks. i lufthavne, hoteller, konferencecentre, caféer eller lignende.

Når du bruger et offentligt trådløst netværk, har du ingen indflydelse på sikkerhedsniveauet på netværket. Sikkerheden på en cafés eller et hotels trådløse netværk afhænger nemlig af, hvad ejeren af det trådløse netværk har indstillet netværket til. Derfor bør du ikke betragte et offentligt trådløst netværk som mere sikkert end at tilslutte sig internettet.

Du bør derfor anvende samme sikkerhedstiltag, som når du tilslutter dig internettet, f.eks. personlig firewall og antivirus på din pc. Derudover bør du bruge kryptering, hvis du skal sende fortrolige data over det trådløse netværk.

Hvad skal du ellers være klar over?

Når du anskaffer et trådløst netværk og har foretaget de sikkerhedsmæssige tilpasninger, er der også andre forhold, du bør være opmærksom på:

Forstyrrelser

Det trådløse netværk bruger typisk frekvenser, som også bruges af mange andre forskellige typer apparater, bl.a. husholdningsudstyr og andet udstyr til datakommunikation. Sådant udstyr kan forstyrre dit trådløse netværk, hvis de to typer udstyr anvendes samtidig. Normalt er forstyrrelserne af kort varighed. Placer dit trådløse netværk så langt fra det forstyrrende udstyr som muligt.

CE-mærke

Dit trådløse netværk skal være CE-mærket. Leverandøren lover med CE-mærket, at dit trådløse netværk sender med den tilladte styrke og bruger de frekvenser, der er afsat til trådløst netværk. CE-mærket garanterer dog ikke mod forstyrrelser.

Yderligere information

For at få hjælp til hvordan du skal indstille dit trådløse netværk, så det sikres bedst muligt, skal du kontakte din leverandør. Der kan være forskel fra det ene trådløse netværksprodukt til det andet, men din leverandør kan fortælle dig, hvordan lige præcis dit udstyr indstilles bedst muligt.

Nogle leverandører tilbyder også VPN, som kan hjælpe til at forbedre sikkerheden i dit trådløse netværk. Spørg din leverandør, hvad de kan tilbyde.

På internationalt plan arbejdes der på at gøre trådløse netværk mere sikre. WPA og WPA2 standarden er et resultat heraf.. Desuden arbejdes der på 802.11x standarderne, så sikkerheden hele tiden forbedres.

IT- og Telestyrelsen følger med i udviklingen. Vi bringer således nyt på vores hjemmeside, når der er nye løsninger på markedet, eller når vi bliver bekendt med nye trusler mod trådløse netværk.

Hos IT- og Telestyrelsen kan du også få andre råd om it-sikkerhed. Nye vejledninger om it-sikkerhed offentliggøres løbende på

www.itst.dk

Ordliste

Basisstation	Basisstationen kaldes ofte for et 'access point' (AP) i manualer og salgsmateriale. Afstanden mellem din pc og AP skal typisk være mindre end 50 - 100 meter, for at du kan få forbindelse.
Broadcast-meddelelse	Information fra et trådløst netværk om navn på det trådløse netværk (SSID), datahastighed og kryptering. Nogle vejledninger bruger andre betegnelser som 'broadcast associations'. Spørg din forhandler, hvis du er i tvivl.
Firewall	En firewall er et program eller en hardware enhed, som regulerer og overvåger adgangen til og fra netværk, f.eks. internettet.
Hacker	Person der uden tilladelse forsøger at trænge ind i en fremmed computer eller netværk.
Kryptering	At gøre data ulæselige ved at forvrænge dem.
SSID	Service Set Identifier (navnet på et trådløst netværk).
VPN	Virtuelt Privat Net - en tjeneste, som laver en sikker virtuel datatunnel fra punkt til punkt for de tilsluttede brugere.
WEP	Wired Equivalent Privacy er den krypteringsstandard, der bruges i de fleste ældre trådløse netværk.
WLAN	Wireless Local Area Network er en engelsk betegnelse for trådløse lokalnetværk.
WPA/WPA2	Wi-Fi Protected Access er en krypteringsstandard, der anvender dynamiske nøgler.

Tjekliste

Hvad du kan gøre for at øge sikkerheden i brugen af trådløse netværk

- [ ] Brug kryptering
- [ ] Slå broadcastmeddelelser fra
- [ ] Skift standard password
- [ ] Skift SSID
- [ ] Benyt en firewall
- [ ] Brug filtrering på MAC-adresser
- [ ] Undersøg Persondatalovens bestemmelser, hvis du håndterer personfølsomme data
- [ ] Er dit WLAN CE-mærket?

Skal du installere et trådløst netværk - hjemme eller i virksomheden?

Har du allerede et trådløst netværk?

Har du tænkt på datasikkerheden i dit trådløse netværk?

Pjecen henvender sig til private og mindre virksomheder, der ønsker en trådløs internetforbindelse, ønsker at koble flere pc'er sammen i et netværk uden brug af kabler eller ønsker at udvide et datanet med et trådløst netværk.

Sikkerhed - hvilke krav skal du stille?

Inden for de sidste par år er trådløse netværk - også kaldet WLAN - blevet meget populære både på arbejdspladsen og i hjemmet. Samtidig har der været fokus på datasikkerheden i trådløse netværk. For signaler fra trådløse netværk kan nå helt ud på gaden, hvor uvedkommende med ganske lidt udstyr kan opfange informationer fra netværket. I værste fald kan uvedkommende få kontrol over din computer og eventuelt ødelægge data.

Ved at følge rådene i denne vejledning er det således muligt at opnå et rimeligt sikkerhedsniveau i dit trådløse netværk.

IT- og Telestyrelsen
www.itst.dk

Rådet for it-sikkerhed
www.raadetforitsikkerhed.dk