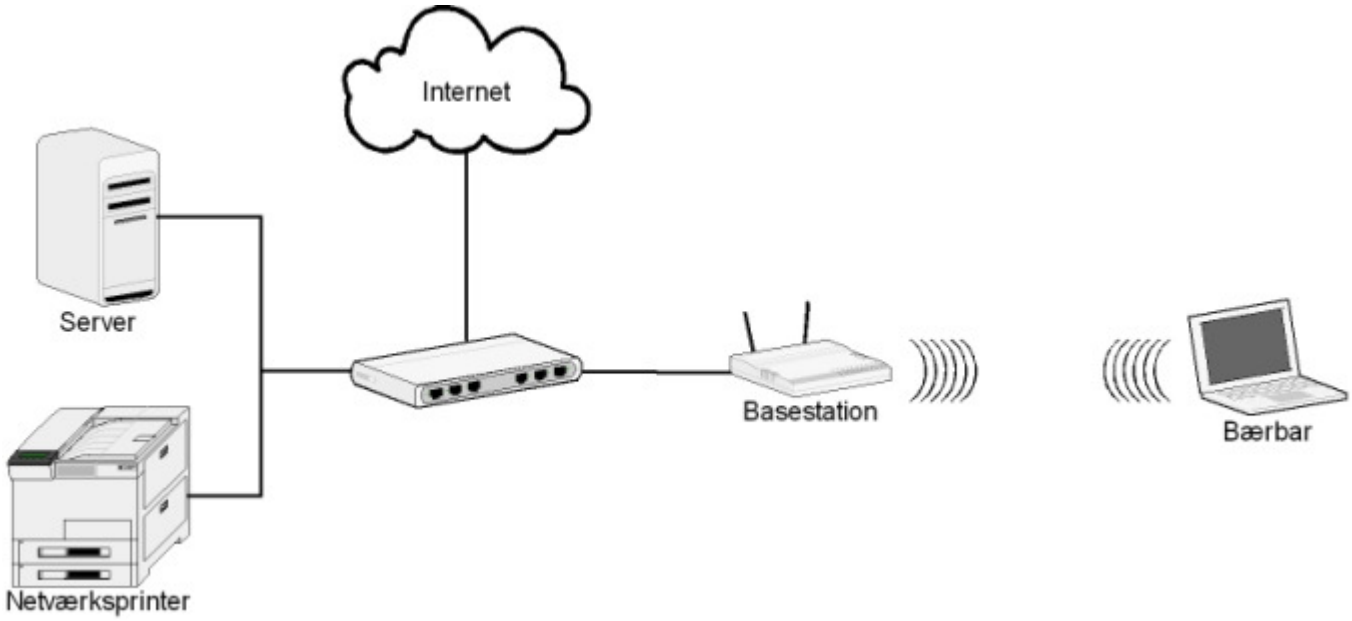
Sikkerhed på trådløse netværk

De senere år er trådløse netværk blevet stadig mere populære. Med en bærbar computer er det muligt at bevæge sig rundt i virksomheden og hele tiden have forbindelse til firmanetværket og / eller internettet.



Et trådløst netværk fungerer ved, at kommunikation mellem PC og basestation sendes via radiobølger. Da radiobølger ikke kan styres på samme måde som kabler i væggen, er det nødvendigt at beskytte sit trådløse netværk mod uindbudte gæster.

Der er forskellige tiltag man kan gøre for at sikre netværket, som i praksis ikke har den store betydning. MAC-adresse filtrering, deaktivering af SSID-broadcast og justering af sendestyrken, gør det lidt sværere at opdage det trådløse netværk og sikrer imod at hvem som helst kobler sig på, men giver ikke nogen egentlig beskyttelse.

Egentlig beskyttelse af det trådløse netværk kan kun opnås med kryptering af den kommunikation der sendes gennem luften og denne artikel omhandler de 3 mest anvendte former.

WEP
WEP (Wireless Equivalent Privacy) er den oprindelige krypteringsform og understøttes i stort set alt trådløst udstyr.

For at forbinde til et trådløst netværk der er beskyttet med WEP, skal der indtastes en krypteringsnøgle på PC'en, som skal være identisk med krypteringsnøglen i basestationen. Længden på krypteringsnøglen kan være 5 tegn (40 / 64 bit) eller 13 tegn (128 bit).

En krypteringsnøgle på 128 bit giver 2^128 forskellige muligheder, så det vil tage millioner af år for en hacker at afprøve samtlige muligheder fra en ende af (kaldet brute-force attack). Desværre er der nogle svagheder i WEP som betyder, at det slet ikke er nødvendigt. Med et program kan hackeren aflytte den trådløse kommunikation og når hackeren har aflyttet tilstrækkelig kommunikation (ca. 300MB), kan krypteringsnøglen knækkes i løbet af få sekunder. På et travlt trådløst netværk tager det under 1 time at indsamle den nødvendige information. Da hackeren udelukkende lytter til andres kommunikation, er det stort set umuligt at afsløre aflytningen.

WPA
WPA (Wi-fi Protected Access) er afløseren for WEP og understøttes i det meste nyere udstyr.

KILDE: http://windows.microsoft.com

Når en bruger forsøger at koble op til et trådløst netværk beskyttet med WPA, er det ikke basestationen der kontrollerer brugeren, men derimod en såkaldt RADIUS-server, som er et program der typisk kører på en server. WPA tilbyder desuden mange forskellige måder hvorpå brugeren kan autoriseres til at bruge det trådløse netværk. Der kan bruges brugernavn / kodeord, engangskodeord, certifikater m.v.

Der bruges, ligesom ved WEP, stadig krypteringsnøgler, men disse udveksles automatisk mellem basestationen og brugerens PC. For en endnu bedre beskyttelse, udskiftes krypteringsnøglerne automatisk løbende - eksempelvis hvert minut.

WPA er dermed meget sikker og - så vidt vides - umulig at bryde, ved kun at aflytte den trådløse kommunikation.

WPA bruges typisk i større trådløse netværk. Da der ikke er nogen fælles krypteringsnøgle, som ved WEP, er det muligt at tildele gæster, eksterne konsulenter m.v. adgang til det trådløse netværk, uden at skulle ændre krypteringsnøgler for alle andre bagefter.

WPA er blevet endnu mere sikker med vedtagelsen af standarden WPA2. Dette understøttes dog kun i det nyeste udstyr.

WPA-PSK
WPA-PSK (Wi-fi Protected Access Pre-Shared Key) er en mellemting mellem WEP og WPA, som kombinerer sikkerheden fra WPA med enkelheden fra WEP.

Ved WPA-PSK skal der indtastes en krypteringsnøgle på PC'en - ligesom ved WEP. Krypteringsnøglen kan dog være noget længere, 63 tegn (256 bit), og sikres på samme måde som WPA ved den trådløse kommunikation. Krypteringsnøglen bør være på mindst 20 tegn, da den ellers kan være sårbar overfor brute-force attacks. Da brugerkontrollen foretages i basestationen, ved sammenligning af krypteringsnøglerne, er der ikke behov for en RADIUS-server.

WPA-PSK bruges typisk af private og i mindre trådløse netværk.

Ligesom der er vedtaget en WPA2 standard er der også vedtaget en WPA2-PSK standard, som understøttes i det nyeste udstyr.

Mere information om trådløse netværk:
http://windows.microsoft.com/da-DK/windows-vista/Wireless-networking-frequently-asked-questions