

STOPP TRUSLENE FØR DE NÅR PC-EN:

Nå blir ruterene enda sikrere

Den nyeste rutergenerasjonen som finnes i butikkene, har innebygd beskyttelse mot hackere, virus, nettfiske og andre trusler. Det gir bedre sikkerhet for alle enhetene på det lokale nettverket.



Journalist
Henning Rasmussen

Hittil har forsvarsverkene mot ondsinnede nettsider, falske annonser, virus og nettfiske stort sett begrenset seg til sikkerhetsprogramvaren du selv har installert på maskinen. Nå er det imidlertid mange produsenter som bygger inn avanserte sikkerhetsfunksjoner i de trådløse ruterne. Det skjer som regel i samarbeid med en anerkjent produsent av sikkerhetsprogrammer og uten at det nødvendigvis koster noe ekstra.

Hvis du for eksempel kjøper en router fra TP-Link, riktignok i en litt høyere prisklasse, kan du få sikkerhetspakken HomeCare med på kjøpet. Det er en løsning fra antiviruselskapet Trend Micro og omfatter foreldrekon-

troll, antivirus og beskyttelse mot de fleste truslene på nettet. HomeCare-beskyttelsen er inkludert i prisen og oppdateres i hele produktets levetid.

Hos Asus ivaretas rutersikkerheten av noe som kalles AIProtection. Også dette er en beskyttelse som leveres av Trend Micro. Tjenesten er inkludert i prisen og finnes blant annet i Asus RT-AX5400 til knappe 2000 kroner.

Netgear-rutere kan på sin side ha sikkerhetspakken Armor, som leveres av Bitdefender. Den beskytter alle nettverksenheter mot virus, spionprogrammer, løsepengevirus og farlige lenker, samtidig som du får en integrert VPN-tjeneste, riktignok begrenset til 200 MB per dag.

Også fra tjenesteleverandørene

Hittil har tommelfingerregelen vært at ruterne man får fra nettselskapene

sjelden har vært blant de beste. "Har du router selv, eller vil du ha en fra oss?" var spørsmålet en kollega nylig ble stilt da han fikk installert fiber-nett. Vi nevner ikke navn, men installatøren la ikke skjul på hva han mente om ruterne han kunne tilby. Også dette vil endre seg etter hvert som ruterne fra nettselskapet kan fungere som salgsargument. I mellomtiden må vi selv sørge for å sjekke ruterne som følger med når vi velger ny nettleverandør eller nytt abonnement.

Enten du kjøper router selv eller får en fra den som leverer internett, er det flere ting du bør undersøke.

Det ser vi nærmere på i denne artikkelen. Vi viser også deg som ikke er innstilt på å kjøpe ny router eller bytte leverandør akkurat nå, hvordan du sikrer ruterne du har i dag så godt det lar seg gjøre.





**Full
beskyttelse
allerede
i ruterene**

Slik beskytter den nye ruter generasjonen

Du har nok allerede en grunnleggende beskyttelse mot trusler i ruterne du har i dag, men sikkerheten i de nyeste modellene er langt høyere.

Sikkerhetsstandard	Din nåværende ruter	De nye ruterne
Brannmur	Ja	Ja
Sikkerhetsnøkkel	Ja	Ja
Kryptering med WPA3 og WPS	Ja	Ja
NAT-beskyttelse	Ja	Ja
VPN	Kanskje	Ja
Foreldrekontroll	Nei	Ja
Smart app til mobilen	Nei	Ja
Antivirus	Nei	Ja
Beskyttelse mot farlige nettsider	Nei	Ja
Automatisk fastvareoppdatering	Kanskje	Ja
DNS-blokkering	Nei	Ja

EKSPERT:

Du bør fortsatt bruke sikkerhetsprogrammer

Man kan få inntrykk av, og skulle kanskje tro, at sikkerheten som er integrert i de nye ruterne gjør at man klarer seg uten sikkerhetsprogrammer på pc-en, fordi du allerede er beskyttet før datatrafikken når frem til tilkoblede enheter. Slik er det ikke, ifølge en av verdens fremste sikkerhetsekspert. David Jacoby, som er rådgiver for en rekke store sikkerhetsselskaper og har hacket alt fra skrivere til Mac-maskiner, har selv erfaring på området fra et samarbeid med en svensk nettleverandør.

Han mener at utvidede sikkerhetsfunksjoner i rutere er en god ting, men at kundene må vite nøyaktig hvordan de er beskyttet og hvordan de ikke er det. Han påpeker at det er umulig å oppnå samme beskyttelse fra ruterne som man får med sikkerhetsprogrammer som er installert på selve pc-en. Det er altså viktig å ikke fire på pc-sikkerheten selv om ruterne er en ekstra barriere mot angrep. Han advarer mot å la en enkeltløsning som en sikrere ruter være en hvilepute. Man må fortsatt være årvåken på nettet og blant annet aktivere to-trinnsgodkjenning der det er mulig.



David Jacoby er hacker og anerkjent sikkerhetsekspert.

Nye rutere er mye sikrere

Alle rutere har integrert brannmur og kryptering av all trafikk mellom hver enhet på nettverket. Den utvidede sikkerheten i den nye rutergenerasjonen gir i tillegg flere nye sikkerhetsfunksjoner.

Sikkerhetsnøkkel (passord)

Nyere rutere gjør det mulig å velge et langt og sikkert passord som kan bestå av flere enn ti tegn og omfatte både bokstaver, tall og spesialtegn. De lange og kronglete passordene beskytter ruterens mot endringer i innstillingene, som kan kompromittere sikkerheten på det lokale nettverket.

Brannmur

Den innebygde brannmuren sørger for å blokkere tilkoblinger fra internett til de enkelte enhetene på det lokale nettverket. Denne funksjonen vil hindre at en hacker for eksempel får tilgang til en nettverksdisk eller et overvåkingskamera.

Kryptering med WPA3 og WPS

Den nyeste sikkerhetsprotokollen heter WPA3 og krypterer trafikken mellom ruterens og tilkoblede enheter, slik at ikke data kan snappes opp av uvedkommende. I tillegg bidrar den integrerte WPS-funksjonen til å etablere en sikker forbindelse til nettverket ved at man trykker på en WPS-knapp på tilkoblede enheter som skrivere og annet.

NAT-beskyttelse

Ruterens inneholder en funksjon kalt NAT, som står for Network Address Translation, og som sørger for å maskere IP-adressene til enheter på det lokale nettverket når de kommuniserer med servere på internett.

Antivirus

Ved å samarbeide med sikkerhetsselskaper som F-Secure, Trend Micro, Avira og Bitdefender, kan ruterprodusenter og nettleverandører også tilby virus-søk allerede i ruterens, slik at farlige filer blokkeres før de når frem til pc-en eller andre enheter. Det er også nyttig for utstyr som skrivere og nettverksdisker.



VPN

VPN-funksjonen gjør det mulig for ruterne å opprette en kryptert tilkobling til en server på internett og dirigere all nettverkstrafikken via den. Når du besøker nettsider, vil denne serveren vises som avsenderadresse i stedet for den egentlige IP-adressen din hos nettleverandøren.

Beskyttelse mot farlige hjemmesider

De nye ruterne inneholder en nettbasert løsning fra et anerkjent sikkerhetsselskap som leverer en oppdatert liste over farlige nettsideadresser, som dermed blokkeres av ruterne. Når du prøver å åpne en hjemmeside som er blokkert av ruterne, får du beskjed om at siden ikke er tilgjengelig. Dermed unngår du å bli eksponert for nettfiske eller skadevare fra den samme nettsiden.

Automatisk fastvareoppdatering

De færreste logger seg inn på administrasjonssidene til ruterne med jevne mellomrom for å se etter oppdateringer til ruterens fastvare. Derfor er det viktig at ruterne automatisk sjekker og oppdaterer programvaren selv, når det kommer en ny versjon. Det gjør nemlig at nyoppdagede sikkerhetshull blir tettet raskest mulig.

Foreldrekontroll

De nyeste ruterne inneholder også en foreldrekontroll som blant annet hjelper deg med å sette opp regler for barnas mobiler og nettbrett og sørger for å blokkere hjemmesider de ikke bør ha tilgang til.

DNS-blokkering

DNS er en tjeneste som sørger for å oversette nettsideadresser til IP-adresser, som består av tall. I en del land benyttes tjenesten også til å sensurere uønskede hjemmesider. På nyere rutere kan DNS brukes til å blokkere tvilsomme hjemmesider eller sider som er kjent for å inneholde skadevare og drive med forsøk på nettfiske.

Smart app til mobilen

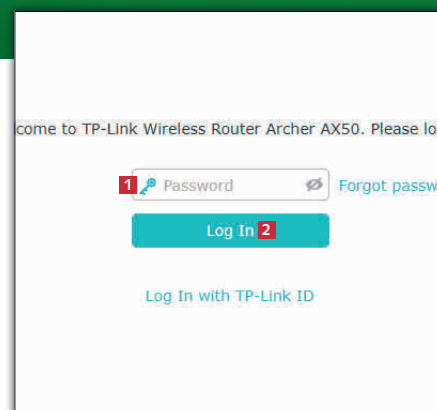
Det er mye lettere å ha kontroll over sikkerheten i ruterne når man har tilgang til den fra en app på mobilen i stedet for å måtte gå via nettleseren på en pc. De nye ruterne gjør det mulig både å justere sikkerheten og å tilpasse den nye foreldrekontrollfunksjonen rett fra mobilappen. Den muligheten gjør at du ikke lenger behøver å huske IP-adressen til ruterne for å ha kontroll over sikkerheten. Appen er koblet direkte til ruterne, og innstillingene endres med det samme.

Slik sikrer du ruterne du allerede har

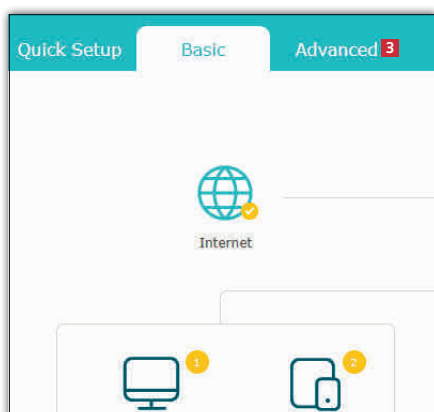
SJEKK SIKKERHETEN I DIN EGEN RUTER

Lukk alle åpne porter!

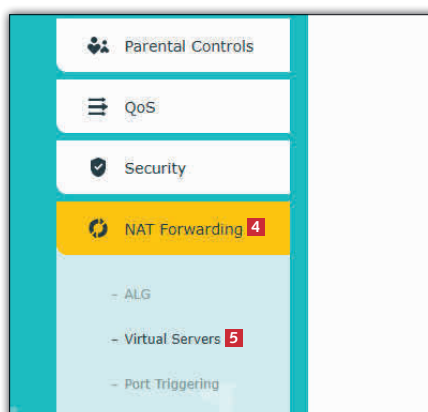
Det er mye du kan gjøre for å forbedre sikkerheten på nettverket selv om du ikke har en av de nye og sikrere ruterne. Alle rutere kommuniserer via porter, og du bør lukke alle porter du ikke selv har åpnet, slik at nettet er så sikkert som mulig. Her ser du fremgangsmåten med en vanlig ruter fra TP-Link, men det vil se omtrent likt ut på andre modeller.



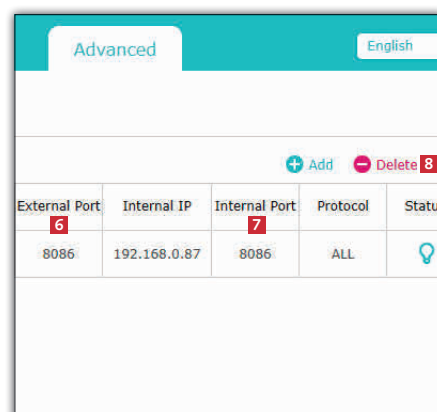
1 Skriv adressen til ruterens i en nettleser. Den står i veiledningen eller på selve ruterens. Oppgi passord **1**, og klikk på **Log In** **2**. Standardpassordet står der du fant adressen.



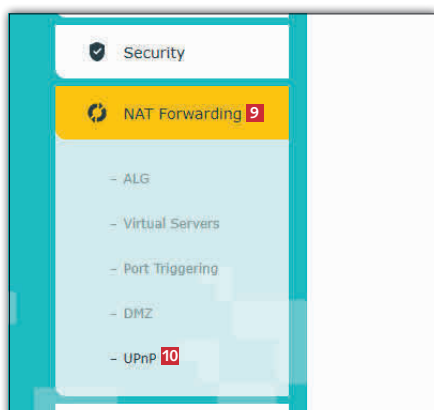
2 Klikk på **Advanced** **3** for å få tilgang til de avanserte innstillingene.



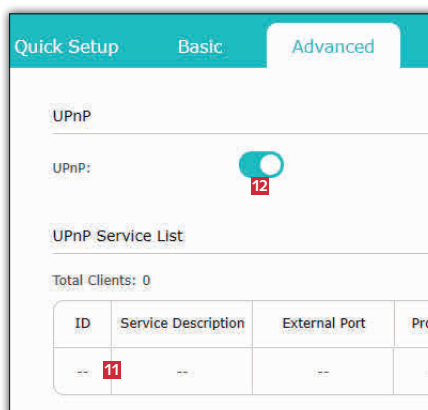
3 Se etter noe som heter for eksempel **NAT Forwarding** **4** eller Port Forwarding. På denne modellen må vi deretter klikke på **Virtual Servers** **5** i menyen.



4 Sjekk om det er lagret regler for videresending av porter **6**. Er det opprettet porter **7** her, bør du slette dem ved å markere regelen og klikke på **Delete** **8**.



5 Under **NAT Forwarding** **9** finner du som regel også punktet **UPnP** **10**, som tillater automatisk tilgang til nettverket for enheter som støtter funksjonen.



6 Hvis du ikke ser tilkoblet utstyr som benytter UPnP-funksjonen **11** aktivt, er det tryggere å slå den av **12**. Det gir bedre beskyttelse.

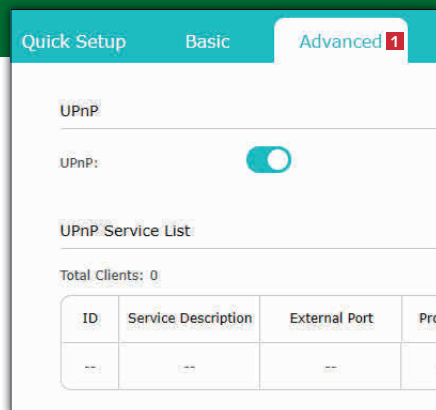
Husk antivirus på pc-en

Enten du har en ny eller eldre ruter anbefaler vi at du installerer det gode antivirusprogrammet Avast One Essential, som du kan laste ned fra komputer.no/2505. Der finner du også en fullstendig veiledning til programmet.

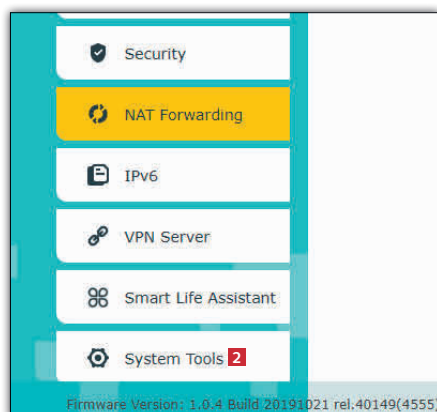


Finnes det oppdateringer?

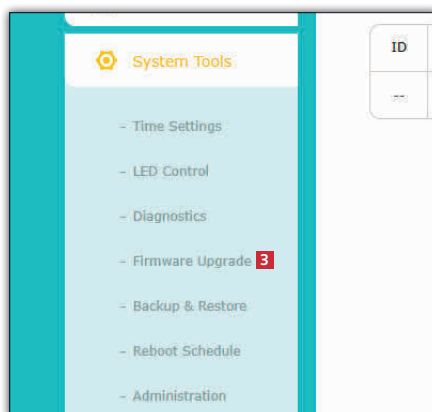
Operativsystemet på en pc oppdateres fortløpende av Microsoft etter hvert som det oppdages nye trusler og sårbarheter. Det samme er ikke nødvendigvis tilfellet for ruterene, og derfor bør du sjekke jevnlig om det finnes oppdateringer av ruterens fastvare. Her ser du hvordan det skjer i en ruter fra TP-Link.



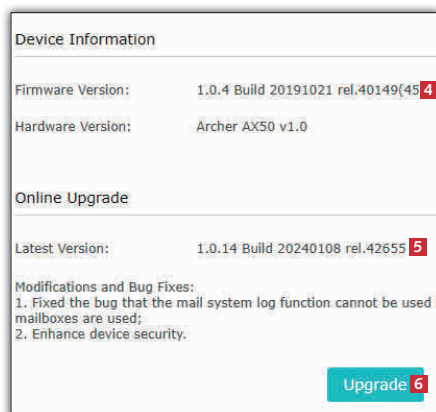
1 Klikk på **Advanced** **1** på kontrollsiden til ruterene for å få tilgang til avanserte innstillinger.



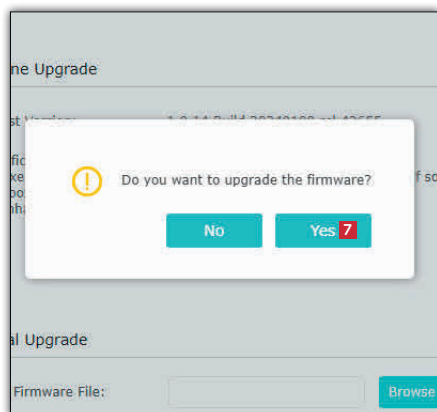
2 Klikk på **System Tools** **2** eller lignende i ruteremenyen.



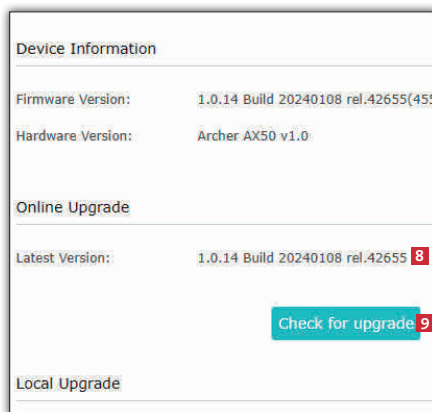
3 Velg **Firmware Upgrade** **3** i undermenyen.



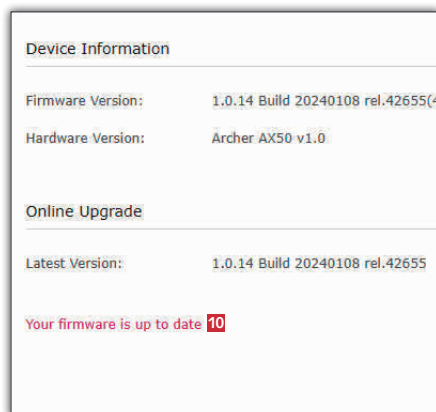
4 Her ser du om den installerte fastvaren **4** kan oppgraderes til en nyere versjon **5**. Klikk i så fall på **Upgrade** **6** for å starte prosessen.



5 Klikk på **Yes** **7** for å fortsette. La være å gjøre noe mer mens oppdateringen pågår. Pc-en vil miste nettverksforbindelsen underveis.



6 Logg på igjen etter 5–10 minutter, og oppdater siden med et trykk på **F5**-tasten. Nå er fastvaren oppdatert **8**. Dobbeltsjekk gjerne med et klikk på **Check for upgrade** **9**.



7 Nå får du vite at fastvaren er den nyeste som finnes **10**, og dermed vet du at du har gjort det du kan for å holde ruterene så sikre som mulig.