

STOP TRUSLERNE, FØR DE NÅR DIN PC:

Nu bliver din router endnu mere sikker

Den nyeste generation af routere, som du kan finde i butikkerne i dag, rummer direkte beskyttelse mod hackere, virus, phishing og andre trusler, så alle enheder på netværket er beskyttede.



Journalist
Henning Rasmussen

I mange år har dit sikre bolværk mod ondsindede hjemmesider, falske annoncer, virus og phishing-angreb været det sikkerhedsprogram, du selv havde installeret på din pc. Men nu er mange producenter af fysisk netværksudstyr begyndt at bygge udvidet sikkerhed ind i de trådløse routere. Ofte i samarbejde med et anerkendt sikkerhedsfirma og umiddelbart uden ekstra omkostninger for dig.

Hvis du køber en router af mærket TP-Link, kan du i den lidt dyrere prisklasse få sikkerhedspakken HomeCare med i købet. HomeCare er en løsning, som leveres af antivirusproducenten Trend Micro og giver dig forældrekontrol, antivirus og beskyttel-

se mod de fleste trusler på nettet. HomeCare er købt og betalt med routeren i hele produktets levetid.

Producenten ASUS kalder deres ekstra router-sikkerhed for AiProtection, og det er en beskyttelse, som også leveres af Trend Micro. Tjenesten er inkluderet i prisen og findes blandt andet i modellen RT-AX5400, der fås til omkring 1.100 kroner.

På vej fra internetudbydere

Routere fra Netgear udleveres ofte af internetudbydere, og her kan du få sikkerhedspakken Armor, der leveres af firmaet Bitdefender, med i købet. Armor beskytter alle dine enheder mod virus, spyware, ransomware og farlige links og giver dig en indbygget VPN-tjeneste, hvor du dog kun må bruge 200 MB om dagen. Den nye trend i routers indbyggede sikker-

hed kan internetudbydere ikke sidde overhørig, og derfor vil du også se flere udbydere lovprise den ekstra sikkerhed, du får med lige præcis deres modemmer og routere.

Hvis du har internet hos YouSee og har fået udleveret routeren Sagemcom FAST380v2 eller FAST380v3, så vil du siden 2023 automatisk have haft sikkerhed indbygget direkte i din router. YouSee har indgået et samarbejde med sikkerhedsfirmaet F-Secure, og har bygget en cloudstyret software ind i routeren, som du selv kan kontrollere via en app til din telefon. Det giver dig browser-beskyttelse, tracking-beskyttelse og IoT-beskyttelse direkte i routeren, så alle dine enheder er skærmet mod truslerne. Indtil videre er kun kunder med internet via kabel-tv-stikket beskyttet, men tilbuddet er på vej til andre kunder også.



Sådan beskytter den nye generation af routere dig

Du har sikkert allerede basal beskyttelse mod trusler i den router, der står i dit hjem, men med de helt nye routere har sikkerheden nået et nyt niveau.

Sikkerhedsstandard	Din nuværende router	De nye routere
Firewall	Ja	Ja
Sikkerhedsnøgle	Ja	Ja
Kryptering med WPA3 og WPS	Ja	Ja
NAT-beskyttelse	Ja	Ja
VPN	Måske	Ja
Forældrekontrol	Nej	Ja
Smart app til din telefon	Nej	Ja
Antivirus	Nej	Ja
Beskyttelse mod farlige hjemmesider	Nej	Ja
Automatisk opdatering af firmware	Måske	Ja
DNS-blokering	Nej	Ja

EKSPERT:

Du har stadig behov for sikkerhed på pc'en

Når YouSee omtaler den nye router-sikkerhed, skriver de, at du med løsningen ikke behøver installere et sikkerhedsprogram på din pc, fordi du allerede er beskyttet, før datatrafikken når dine enheder. Men det mener en af verdens fremmeste sikkerhedseksperter er en dårlig idé. David Jacoby, der er rådgiver for en række store sikkerhedsfirmaer og har hacket alt lige fra printere til Mac-computere, har selv erfaring på området fra et samarbejde med en svensk internetudbyder.

Han fortæller, at ideen om den nye, indbyggede sikkerhed grundlæggende er god, men at kunderne skal sættes ind i præcis, hvor de er beskyttet og hvor de ikke er. Han fortæller, at det er umuligt at give samme beskyttelse fra routeren, som man får, når sikkerheden er installeret direkte på pc'en. Derfor må du ikke slække på pc-sikkerheden, selvom du også får beskyttelse i routeren. Han råder til at udvise stor forsigtighed på nettet og blandt andet at aktivere tottins-verificering, da de sikre routere ikke giver dig komplet beskyttelse.



David Jacoby er hacker og en anerkendt sikkerhedsekspert.

Nye routere er så sikre som Fort Knox

Alle routere er udstyret med en indbygget firewall og kryptering af trafikken mellem hver enhed på netværket, men med den udvidede sikkerhed i den nye generation af routere får du en lang række ekstra sikkerhedsfunktioner.

Sikkerhedsnøgle (adgangskode)

Nyere routere giver dig mulighed for at vælge en lang og sikker adgangskode, der kan rumme mere end 10 tegn og bestå af både bogstaver, tal og tegn. De besværlige adgangskoder beskytter routeren mod ændringer i dens indstillinger, som kan kompromittere din sikkerhed.

Firewall

Routerens indbyggede firewall sørger for at blokere forbindelser fra internettet ind til dine enheder på lokalnetværket. Med denne funktion vil en hacker ikke kunne få adgang til din NAS eller et netværkskamera i entreen.

Kryptering med WPA3 og WPS

Med den nyeste sikkerhedsprotokol WPA3 krypteres trafikken mellem routeren og dine enheder, så data ikke kan opsnappes af uvedkommende. Derudover hjælper den indbyggede WPS-funktion med at etablere en sikker forbindelse til netværket ved at trykke på en knap på en printer, en repeater eller en helt tredje netværksenhed.

NAT-beskyttelse

Din router rummer funktionen NAT, der står for Network Address Translation, og som sørger for at maskere IP-adresserne til dine enheder på det lokale netværk, når de kommunikerer med servere på internettet.

Antivirus

Ved at samarbejde med sikkerhedsfirmaer som F-Secure, Trend Micro, Avira og Bitdefender kan routerproducenter og internetudbydere nu også tilbyde virusscanning direkte i routeren, så de farlige filer er blokeret, inden de når din pc eller andet grej. Det er også nyttigt til udstyr som printere og NAS'er.



VPN

Med funktionen VPN kan din router lave en krypteret forbindelse til en server på internettet og dirigere al din trafik gennem denne server. Når du besøger hjemmesider, vil du så have denne server som afsenderadresse i stedet for din ægte IP-adresse hos internetudbyderen.

Beskyttelse mod farlige hjemmesider

De nye routere rummer en såkaldt cloudløsning fra et anerkendt sikkerhedsfirma, der leverer en konstant opdateret liste over farlige hjemmesideadresser, som dermed blokeres i routeren. På din pc vil du få at vide, at hjemmesiden er utilgængelig, når du forsøger at besøge den i din browser, hvis den er blokeret af routeren. Dermed vil du ikke være eksponeret for phishing eller malware fra siden.

Automatisk opdatering af firmware

De færreste logger jævnligt på routerens styresider og tjekker for nye opdateringer til routerens indbyggede firmware, og derfor er det afgørende, at routeren af sig selv kan kontrollere og opdatere softwaren, når der er en ny udgave. Det betyder nemlig, at nyligt opdagede huller i sikkerheden lukkes hurtigst muligt.

Forældrekontrol

På de nyeste routere finder du også en forældrekontrol, som blandt andet hjælper med at indstille regler for ungerne telefoner og iPads og sørger for at blokere hjemmesider med underlødigt indhold.

DNS-blokering

DNS er en tjeneste, der sørger for at oversætte hjemmesideadresser til IP-adresser, der består af tal, og tjenesten bruges også i visse lande til at censurere uønskede hjemmesider. På nyere routere kan DNS bruges til at blokere for underlødige hjemmesider eller hjemmesider, der indeholder malware og phishingforsøg.

Smart app til din telefon

Det er meget nemmere at indstille sikkerheden i routeren, når det kan foregå fra en app på telefonen i stedet for den slagne vej i pc'ens browser. De nye routere giver dig mulighed for både at justere sikkerheden og at indstille den nye funktion forældrekontrol direkte fra app'en på din telefon. Med den mulighed behøver du ikke huske en besværlig adresse til routeren for at justere på sikkerheden. App'en er koblet direkte til din router, og indstillingerne træder straks i kraft.

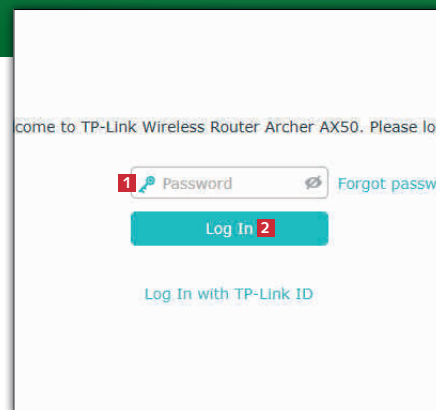
Sådan sikrer du den router, du allerede har



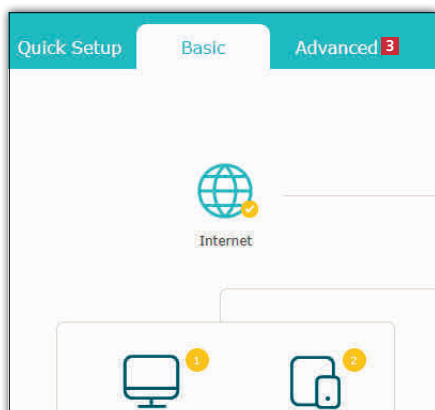
TJEK SIKKERHEDEN I DIN EGEN ROUTER

Luk din routers åbne porte

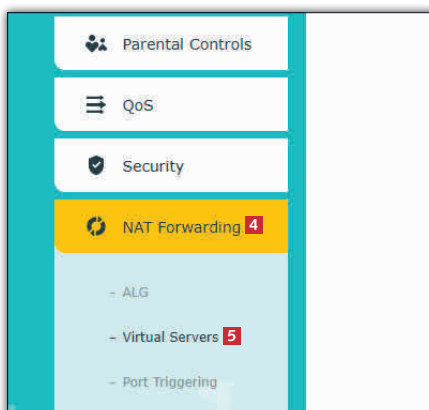
Selv om du ikke ejer en af de nye og sikrere routere, kan du stadig forbedre sikkerheden på dit netværk. Alle routere kommunikerer via porte, og du bør lukke for alle porte, som du ikke selv har åbnet, for at gøre værnet mod internettet stærkere. Det viser vi her i en almindelig router fra firmaet TP-Link, men det vil se nogenlunde tilsvarende ud i andre routere.



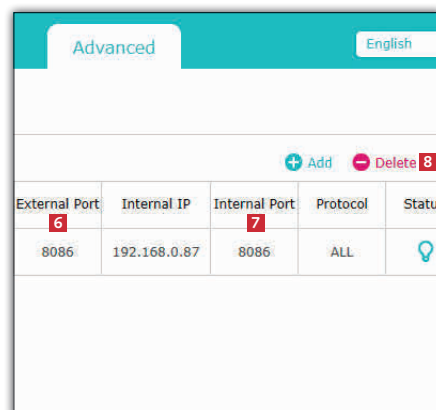
1 Åbn din browser og skriv adressen til din router. Den står i manualen. Tast koden til routeren **1** og klik på **Log In 2**. Standardkoden til routeren står også i manualen.



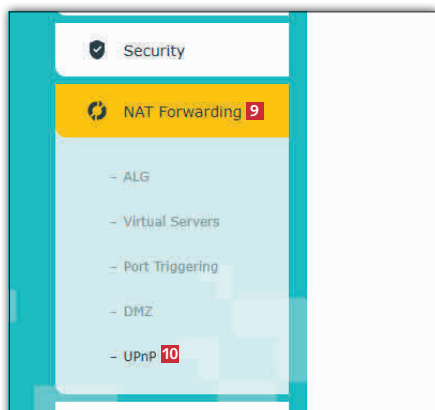
2 Klik på **Advanced 3** for at få adgang til routerens avancerede indstillinger.



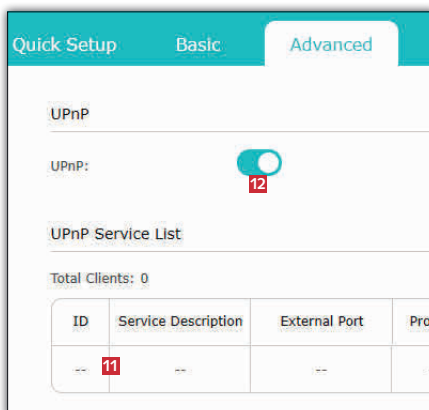
3 Find nu et punkt, der hedder fx **NAT Forwarding 4** eller Port Forwarding. På denne model skal du derefter klikke på **Virtual Servers 5**.



4 Tjek om der er gemt regler for videresendelse af porte **6**. Hvis der er oprettet porte **7** her, bør du slette dem ved at markere reglen og klikke på **Delete 8**.



5 Under **NAT Forwarding 9** finder du som regel også punktet **UPnP 10**, der tillader automatisk adgang til netværket for enheder, der virker med det.



6 Hvis der ikke vises tilkøbtet udstyr i listen, som aktivt bruger UPnP-funktionen **11**, er det mere sikkert at slå den helt fra **12**, så dit netværk er bedre beskyttet.

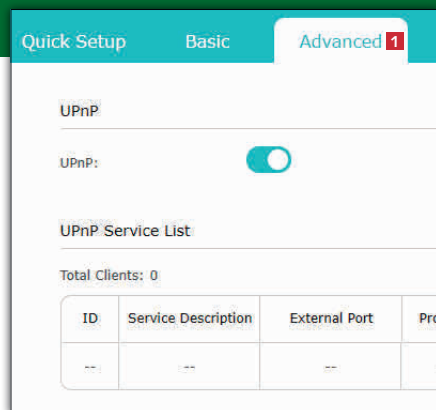
Husk antivirus på din pc

Uanset om du har en ny router anbefaler vi, at du installerer det fremragende antivirusprogram Avast One Essential, som du kan hente på komputer.dk/2505. Her finder du også den komplette guide til programmet.

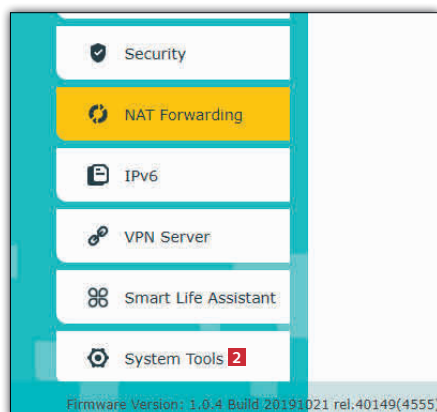


Er der nye opdateringer til din router?

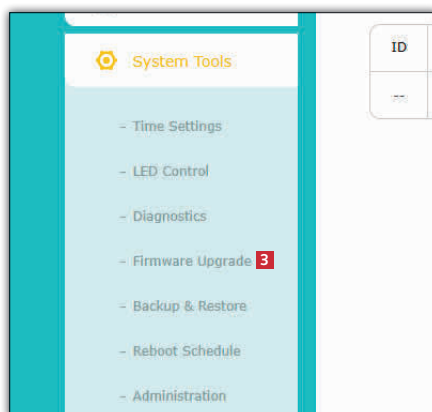
Din pc's styresystem bliver løbende opdateret af Microsoft, når der opdages nye sikkerhedshuller og andre farer. Det samme er ikke nødvendigvis tilfældet for din router, og derfor bør du jævnligt tjekke, om der findes opdateringer til dens firmware. Her viser vi, hvordan du gør i en router fra TP-Link.



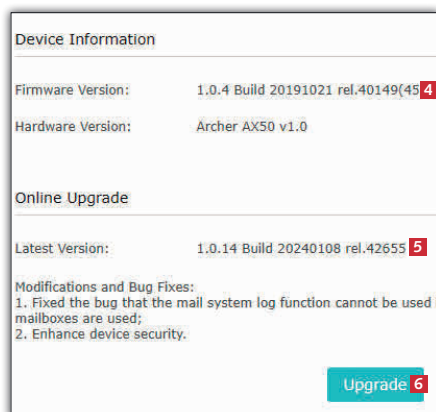
1 Klik på **Advanced** **1** inde i routerens styresider for at få adgang til routerens avancerede indstillinger.



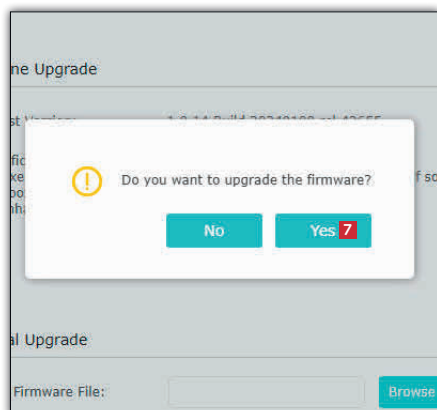
2 Klik på **System Tools** **2** eller lignende i routerens menu.



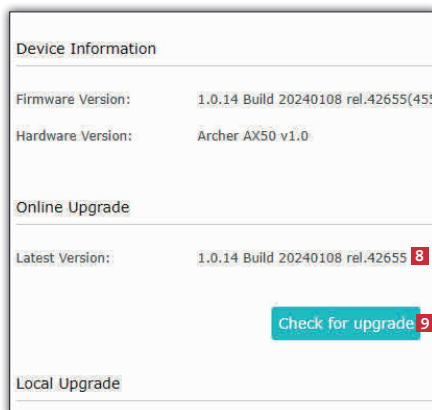
3 Vælg nu punktet **Firmware Upgrade** **3** i undermenuen.



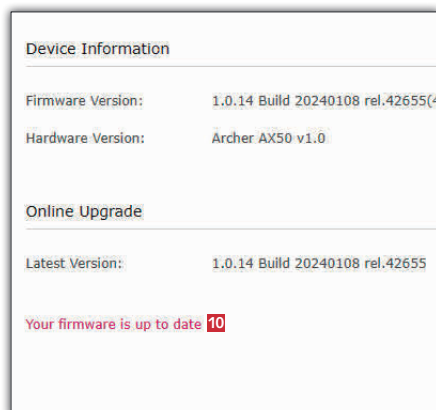
4 Her vil du se, hvis den installerede firmware **4** som her kan opgraderes med en nyere udgave **5**. Klik på **Upgrade** **6** for at opdatere routeren.



5 Klik nu på **Yes** **7** for at fortsætte. Undlad herefter at pille ved din router, mens den opdaterer. Undervejs vil din pc blive frakoblet netværket.



6 Log på netværket efter 5-10 minutter og opdater siden med **F5**-tasten. Nu er firmwaren opdateret **8**. Du kan klikke på **Check for upgrade** **9** for at dobbelttjekke.



7 Så får du besked om, at routerens firmware er den senest tilgængelige **10**. Nu har du producentens seneste sikkerhedsrettelser installeret.