3.6 Säkerhetsfunktioner i Windows

Datavirus

Datavirus är små program som har skapats av en person i syftet att infektera filer i en dator, att sprida sig till andra datorer och att tillfoga skada i den smittade datorn. Med att ”infektera filer” menas att gömma virusets programkod i filen som i regel fortsätter att fungera som vanligt, men har blivit lite större. Detta för att spridas till andra enheter via e-post, USB-minnen, Internet, lokala nätverk osv. Oftast är viruset programmerat att aktiveras vid vissa händelser som t.ex. start resp. omstart av datorn, andra händelser eller vid vissa fastlagda tidpunkter. Den här typen av datavirus kallas för *egentliga datavirus*.

Det finns tre olika typer av datavirus: *egentliga datavirus*, som beskrevs ovan, *Trojaner* och *Maskar*. Trojaner är program som användare luras att installera i datorn och som innehåller kod som utnyttjar säkerhetshål i systmet, för att öppna datorn för intrång utifrån. Dvs andra personer kan sedan komma åt innhållet i datorn och göra i princip vad som helst. Maskar är små program som i sig inte gör någon skada, utan sprider och förökar sig snabbt och kan överbelasta datorn. Maskar kommer in i datirn via säkerhetshål i systemet.

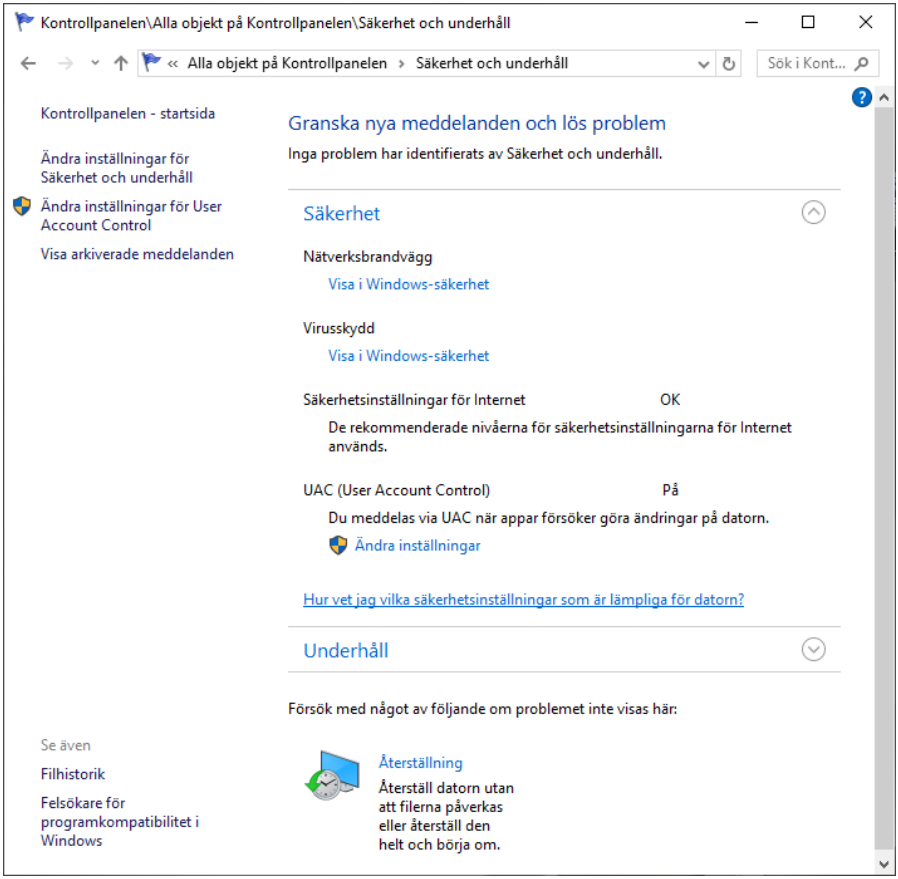
Antivirusprogram

Det är program som kan upptäcka och oskadliggöra datavirus, trojaner och maskar. De har oftast flera funktioner: De kan söka igenom datorn efter eventuella virus, isolera dem genom att försätta dem i karantän eller ta bort dem. De kan också kontrollera alla nya filer samt e-post som kommer in. För att göra det måste antivirusprogram vara utrustade med de nyaste virusdefinitionerna bestående av kända virustyperna som sprids på Internet. Det finns en uppsjö av mer eller mindre kända antivirusprogram med olika prestanda. I Windows finns det inbyggda antivirusprogram som vi ska titta på.

Kontrollpanelen – Säkerhet och underhåll

Ikonen *Säkerhet och underhåll* i Kontrollpanelen leder till ett fönster. Klickar man vidare på resp. pil i högerkanten visas följande detaljer:

Avsnittet *Säkerhet* omfattar följande detaljer:



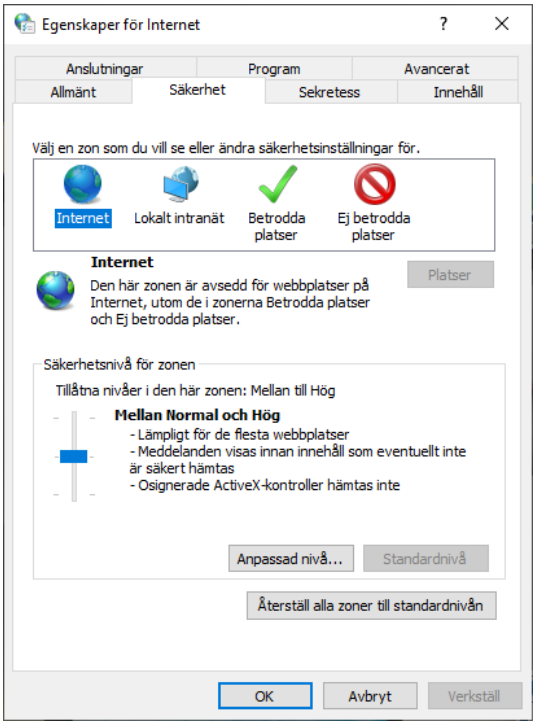
Nätverksbrandvägg anger vilka brandväggsprogram som är installerade. I Windows finns det ett inbyggt brandväggsprogram som blir avaktiverat om man installerar ett särskilt eget program. Två olika brandväggsprogram kan krocka med varandra. Samma gäller för virusskyddsprogram.

Virusskydd anger om datorn har något virusskyddsprogram installerat. Om inte, får man en kritisk varning.

UAC (User Access Controll) meddelar när appar försöker göra ändringar på datorn. Detta för att hindra andra användare än administratörer att ändra viktiga inställningar i datorn.

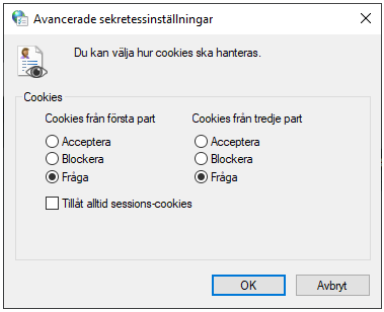
Säkerhetsinställningar för Internet

Ikonen *Internetalternativ* i Kontrollpanelen leder till ett fönster. Klickar man vidare på fliken *Säkerhet* visas följande detaljer:



Här kan man ange vilken säkerhetsnivå man vill ha för olika zoner. Zonerna är uppdelade i: Lokalt intranät, Betrodda platser och Ej betrodda platser. Vilka platser som ingår i de två sistnämnda kan man själv styra genom att klicka på knappen *Platser* och ange webb- resp. ip-adresser som ska ingå i resp. zon. Zonen Lokalt intranät är samma som det lokala nätverket och zonen Internet är alla andra platser som inte ingår i någon av de övriga.

Väljer man i fönstret till höger fliken *Sekretess* kan man ange sekretessnivå, dvs vad som ska gälla angående vad din dator lämnar ut för information till webbsidorna och vad som sparas på din dator. *Cookies* är ett exempel på detta. Klickar man i fliken *Sekretess* på knappen *Avancerat* kan man välja hur Cookies ska hanteras. Vill man vara restriktiv kan man t.ex. göra inställningarna till höger:

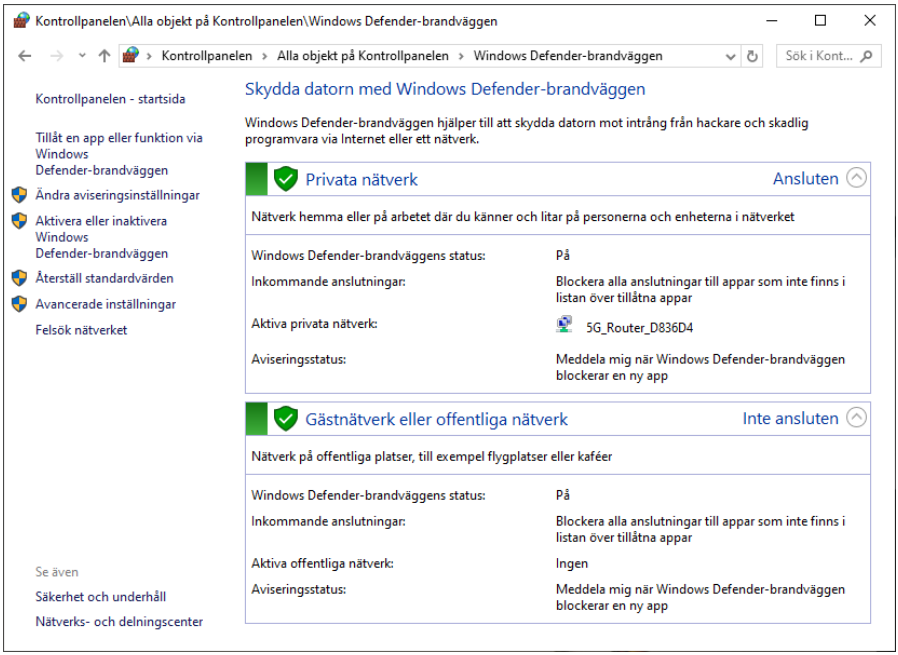


Bakom knappen *Inställningar* i fliken *Sekretess* kan man också blockera *popup-fönster*.

Under fliken *Innehåll* kan man bl.a. hantera *Certifikat* som är inlagda i datorn. Certifikat är äkthetsbevis för programvara som utfärdas av tillverkarna för att förhindra att piratkopior sprids.

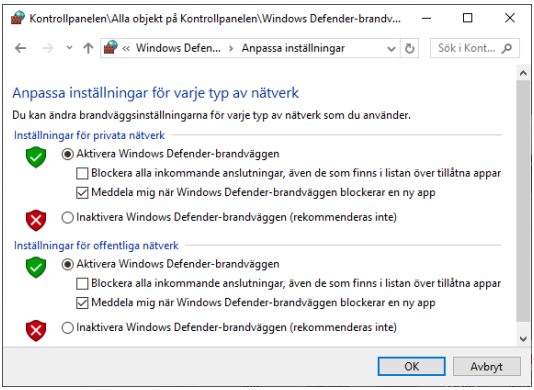
Windows-brandväggen

Ikonen *Windows Defender-brandväggen* i Kontrollpanelen leder till följande fönster:



Denna programvara som är inbyggd i Windows ska skydda datorn mot intrång både från hackare och appar som via Internet eller lokala nätverk försöker att installeras på datorn. En egen tredjepart brandvägg får inte användas då denna krockar med Windows brandvägg.

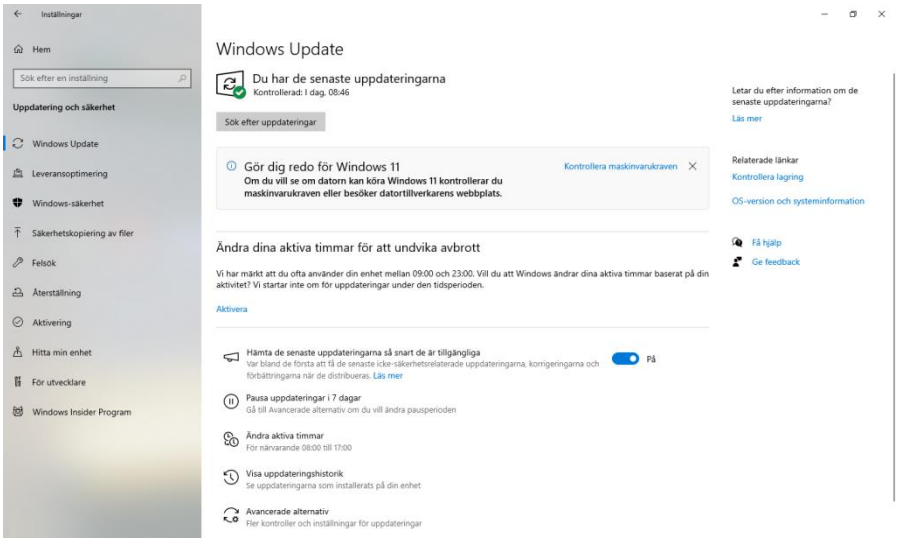
Man kan konfigurera Windows brandvägg med olika inställningar för olika nätverkstyper: *Privata nätverk*, *Offentliga nätverk* och *Företagnätverk*. En standardinställnig är alltid konfigurerat vilket visas i fönstret ovan. Den viktigaste inställningen är att den är *På*. Vill man ändra detta klickar man i vänsterspalten på *Aktivera eller inaktivera Windows Defender-brandväggen.* Man kommer till fönstret *Anpassa inställningar:*



Här kan man bl.a. inaktivera brandväggen för de olika typerna av nätverk och göra andra inställningar.

Windows Update

Ikonen *Uppdatering och säkerhet* i *Inställningar* leder till fönstret *Windows Update:*



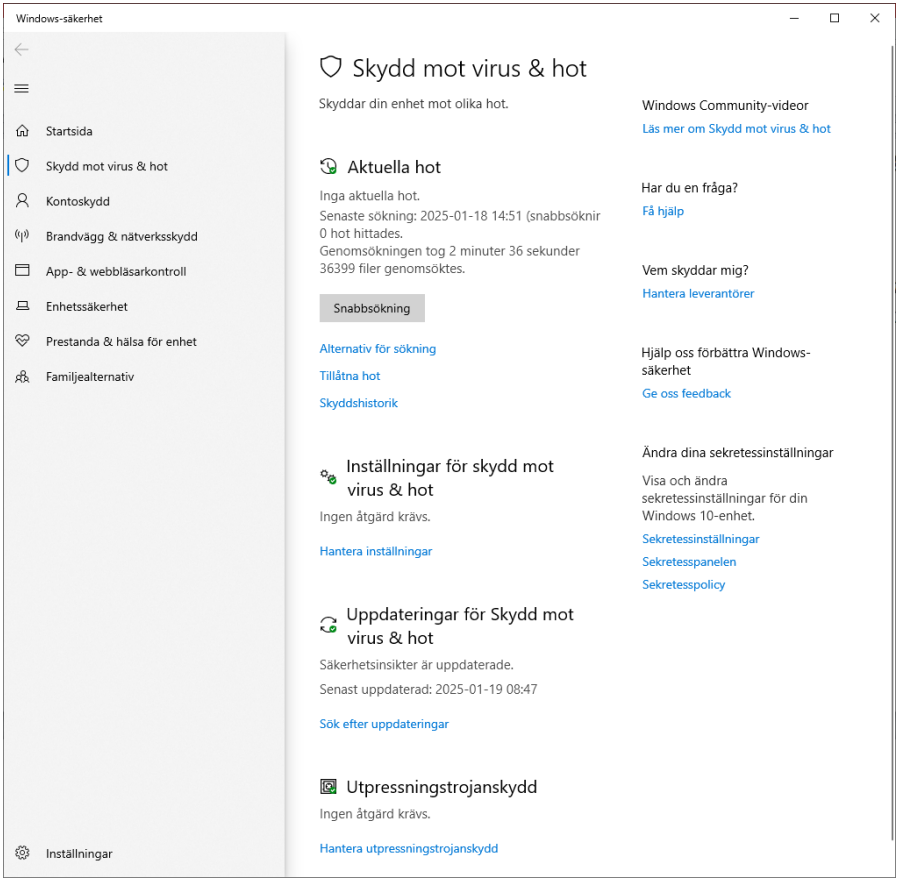
Här har man samlat de flesta funktioner och inställningar för datasäkeher i Windows. *Windows Update* är den funktion i Windows som svarar för att operativsystemet hålls uppdaterat med senaste buggfixar, säkerhetsuppdateringar, drivrutiner och programvaror. Här får man information om bl.a. vilka uppdateringar som är installerade och om det finns tillgängliga uppdateringar som vätar på att installeras. Det finns obligatoriska och valfria uppdateringar. Normalt letar datorn automatiskt efter tillgängliga uppdateringar. Men man kan göra det även manuellt.

Klickar man på *Visa uppdateringshistorik* kan man granska vilka uppdateringar som utförts. Det finns även möjligheten till att avinstallera vissa uppdateringar om man tycker att de snarare ställer till problem.

Windows Defender

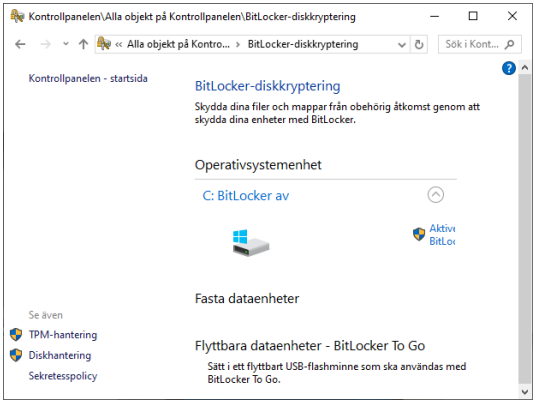
Klickar man i *Windows Update* (ovan) i vänsterspalten på *Windows-säkerhet* och väljer *Skydd mot virus och hot*, kommer man till det inbyggda Antivirus-programmet i Windows som även har namnet *Windows Defender*, se nästa sida. Förutom att skydda mot vanliga datavirus så har det även skydd mot spionprogram, s.k. *Trojaner* och annan skadlig programvara.

Den viktigaste funktionen i Windows Defender är *Snabbsökning* som letar efter aktuella hot och visar resultatet på bara några minuter. En automatisk uppdatering av de senaste virusdefinitionerna ingår i programmet.



BitLocker-diskkryptering

BitLocker-diskkryptering i Kontrollpanelen (till höger) är ett krypteringsverktyg som kan kryptera hela hårddisken. Varianten *BitLocker To Go* kan kryptera flyttbara enheter som USB-minnen.



Besvara nu frågorna 3.195-3.206 på sid 104 om avsnitt 3.6 Säkerhetsfunktioner i Windows.