

## Sikkerhet

**Sikkerhet ? et vanskelig tema. Vanskelig fordi meninger lett blir beskyldt for å være påstander, som f.eks. at "Linux er sikrere enn Windows". En påstand eller et faktum? Uansett påstand eller faktum, så må et slikt utsagn begrunnes, og da blir det fort svært teknisk. Jeg er ingen sikkerhetseksperter, men jeg er i stand til å lytte til en del av de som jobber med og er opptatt av sikkerhet. Så istedet for å hevde hva jeg selv mener, vil jeg her forsøke å lage lenker til informasjon om sikkerhet knyttet til Linux og fri programvare generelt og forsøke å forklare det sikkerhetmessige rundt Linux og fri programvare.**

I en analyse fra Helge Skrivervik (IT-rådgiver/analytiker/strateg som driver rådgivnings-/analysenettstedet [mymayday.com](http://mymayday.com)) hevder han at Storm-ormen kun infiserer Windows-maskiner. Dette hevdes også av andre:

- [In millions of Windows, the perfect Storm is gathering](#)
- [Storm Worm Dwarfs World's Top Supercomputers \(Washington Post\)](#)
- [Wikipedia om Storm](#)

Storm ormen utnytter altså svakeheter, «huller», i Windows operativsystemet, noe dessverre Windows er mer plaget med enn f.eks. Linux. Dette har med den grunnleggende oppbyggingen av operativsystemet. Noen ganger oppdager folkene bak Storm et slikt sikkerhetshull (en svakhet) før Microsoft eller deres partnere selv oppdager det, mens andre ganger oppdages det først av Microsoft. Det som da skjer er at Microsoft gir ut en sikkerhetsoppdatering som brukerne selv må installere. samtidig vil også sikkerhetsleverandøren av sikkerhetsløsningen («antivirus-programmet») komme med en sikkerhetsoppdatering. Begge deler tar tid. Blant de systemene som driftes av profesjonelle IT-personer, så gjøres dette rent rutinemessig. Resultatet er at servere (tjenermaskinene) i liten grad, om enn i det hele tatt, blir infisert.

Dette vet de som lager slik uønsket/fiendtlig kode. Derfor er f.eks. Storm utelukkende rettet mot sluttbrukernes PC-er. Hvor flinke er de til å oppdatere sin maskin med sikkerhetsoppdateringene? Og hvor flinke er de til **ikke** å klikke på vedlegget til en «spennende e-post»? (som er hovedmåten Storm blir spredt på)

Mange hevder at det bare er et tidsspørsmål om når slik fiendtlig kode også blir laget for Linux. Dette er en påstand som krever svært inngående, teknisk

kompetanse for å svare på. Blant fagfolk innenfor operativsystemer og sikkerhet, så er det hevet over enhver tvil at Unix og dens mange varianter (som Linux og BSD) er bygd opp på en slik måte at de faktisk rent teknisk er vesentlig sikrere. Men jeg har erfart, dessverre, at mange ikke aksepterer dette, og ser på det kun som en påstand. Jeg vil derfor komme med lenker til artikler/publikasjoner som kan underbygge dette faktum.

Wikipedia har [denne oversikten over operativsystemer som har fokus på sikkerhet](#), og som regnes som svært sikre, og har også en [oversikt over sikkerhetsnivåene](#) til en del kjente operativsystemer.

Ondsinnede tradisjonelle exe-fil-virus, dvs. virus som infiserer andre programmers kjørebare binærfiler, har aldri eksistert for GNU/Linux. I dag brukes ordet virus om en rekke forskjellige typer ondsinnet programvare og man må skille på de forskjellige typene.

Det finnes ingen effektive *ormer* til GNU/Linux pr dags dato og det er langt vanskeligere å skrive *droppers*, som er den delen av ormen som infiserer systemet ditt og som vanligvis er tradisjonelle exe-fil-virus.

Selv om det er mulig å skrive trojaner, er det få Trojaner som også er langt vanskeligere å spre på GNU/Linux, se [Wikipedias virus-statistikk](#) for forskjellige operativsystemer.

Du har kanskje hørt argumentet om at GNU/Linux ikke er like utbredt som andre operativsystemer og derfor ikke har like mange virusplager? Det er riktig at GNU/Linux ikke er like utbredt, men at det er årsaken til at man ikke plages like mye av virus er feil. GNU/Linux vil aldri vil få tilsvarende virusplager som man kan oppleve i visse proprietære operativsystemer. Du kan [lese hvorfor her](#) eller [en teoretisk forklaring her](#).

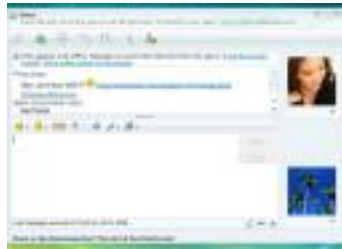
GNU/Linux baserer seg blant annet på sikkerhet gjennom [Linus' lov](#) i motsetning til proprietære systemer som baserer seg på en tro om at [ukjente sikkerhetshull ikke vil bli utnyttet](#).

De eneste exe-fil-virusene som noen gang har eksistert for GNU/Linux har vært laboratorievirus. Det er helt utenkelig at noen slike virus noen gang kunne få en [grobunn i GNU/Linux](#), særlig på grunn av måten programmer installeres og kjøres. Noe som også fjerner motivasjonen for å skrive slike virus fullstendig. Samtidig er det å skrive den typen virus for GNU/Linux vanvittig avansert, på linje med å skrive sin egen exefil-kompilator, i [motsetning til andre proprietære operativsystemer](#).

### **Spyware, Adware eller annen slags Malware sniker seg ikke inn på GNU/Linux.**

Dersom du benytter GNU/Linux, dvs. utelukkende fri programvare, er det helt utenkelig at du vil oppleve noe spyware eller adware overhode, noen gang, uansett hvor mange brukere plattformen GNU/Linux får. For hvordan skal noen kunne klare å lure deg til å installere slikt da?

### **Microsofts MSN-tjeneste ? en kilde for spredning av ondsinnet kode**



Gjennom MSN spres ofte mye ondsinnet kode. Ungdom i alderen 13-19 er nysgjerrige på så mangt, og har kanskje begrenset kunnskap om IT-sikkerhet. Får man en melding fra noen som man kjenner, så kan det jo være fristende å klikek på den lenken som fulgte med meldingen. Og vips, så var man infisert. Overskriften «ENDA et MSN-virus?» i Computerworld.no den 24. januar 2008 er illustrerende; **«ENDA et...». I don't say anymore.**