Sagde du virus?

Ofte benyttes betegnelsen ”virus” om alle former for skadelig kode, men det er ikke helt korrekt.

Af Erik Jon Sloth 21/02-2003 (http://sikkerhed.tdconline.dk)

Det kan være fristende bare at kalde alle former for skadelige programmer for "virus", men i virkeligheden findes der flere forskellige typer af skadelig kode. Viruseksperter kalder koden noget forskelligt alt efter hvilke egenskaber, den har, men de mere udspekulerede typer benytter en kombination af egenskaberne, og det har været med til at gøre forvirringen total. Ofte benytter man bare betegnelsen ”virus” for alle former for skadelig kode, men det er ikke helt korrekt.

Herunder kommer en kort beskrivelse af de overordnede kendetegn ved forskellige typer af skadelig kode.

Virus
En virus hedder en virus, fordi den minder om en forkølelse. Den er nødt til at have en krop at leve i - for eksempel et tekstbehandlingsprogram, et mailprogram eller et Word-dokument - og den har egenskaber, der gør den i stand til at sprede sig selv.

Når du starter det inficerede program eller åbner dokumentet virker alt normalt, men bagved er virussen også blevet startet. Nu kan virussen så gøre ting og sager, uden at du opdager det. Ofte vil virussen inficere andre programmer eller dokumenter på computeren, og måske sørge for at inficere programmer, der startes, når computeren tændes. På den måde vil den blive spredt til andre computere, hvis du sender programmer eller dokumenter til andre eller har delte mapper på din computer, som andre har adgang til.

Virussen nøjes desværre ofte ikke med at sprede sig. Den kan slette filer på harddisken, for eksempel på en bestemt dato, eller den kan sende tilfældige dokumenter fra din harddisk til en bestemt e-mail-adresse.

Hvis virussen har inficeret et program, er der i praksis ingen grænser for, hvad den kan, når først den kører. Den har adgang til de samme ting på computeren som dig, hvilket ofte vil sige, at den har adgang til alt.

Hvis virussen har inficeret et Word-dokument eller lignende, kan det være lidt sværere for den, for så har den kun adgang til funktioner på computeren som ligger i Word. Her er det et problem, hvis du ikke har hentet de seneste sikkerhedsopdateringer fra Microsoft, for så kan der være huller, virussen kan udnytte til at få kontrol over din maskine.

Virusser eller vira?
Hvad hedder det så, når der er mere end een virus?

Ifølge Dansk Sprognævn er både "virus", "virusser" og "vira" korrekte flertalsformer af "virus" på dansk. Da virus oprindeligt er et masse-ord, som reelt ikke kan bøjes på latin (der er ikke noget, der hedder "vira"), opfordrer vi til at udbrede brugen af det mere danskklingende "virusser".

Se Retskrivningsordbogen om virus.
Se også en grundigere forklaring om ordet "virus".

Orm
En Orm minder om en virus, men ormen er et selvstændigt program, som ikke har brug for et andet program for at blive spredt. Den inficerer derfor heller ikke programmer på din computer, men lever i det skjulte, og sørger ofte for at blive aktiveret som en del af opstarten, når du tænder computeren, eller når du starter bestemte programmer. En orm skal altså ikke ændre i programmerne på din computer for at overleve, som en virus gør.

Den spreder sig ved at udnytte huller i sikkerheden i Windows, på servere, i din browser eller ved at udnytte, at mange stadig ikke har lært at være forsigtige, når de modtager en fil med en spændende titel som for eksempel ”who_shot_JFK.vbs”. Igen er det vigtigt, at du har de seneste sikkerheds-opdateringer fra Microsoft. Ellers er der risiko for, at en orm udnytter svagheder i din browser, som gør, at du kan blive angrebet, hvis du surfer forbi en hjemmeside, der er inficeret af en orm.

Når ormen har inficeret en maskine, spreder den sig selv ved udsende e-mails, der indeholder kopier af ormen, ofte til alle i dit adressekartotek, eller ved at benytte din internetforbindelse til at søge efter andre maskiner med huller i sikkerheden, som den kan inficere. Ligesom virus kan orme også forvolde store skader ved at slette filer, men en anden kedelig egenskab er, at de mest aggressive orme spreder sig i så store mængder, at de får dele af internettet til at køre langsommere, eller helt lammer en virksomheds kommunikation, fordi mailserverne overbelastes.

Trojanske heste
En trojansk hest er ikke en egentlig virus, men blot en egenskab ved en virus eller en orm.

Når en orm installerer en trojansk hest på offerets computer, er der skabt en ”bagdør”, som kan udnyttes til at styre computeren udefra. Den trojanske hest kan nu enten sende en besked ud i verden, så en ondsindet person kan få at vide, at computeren er klar til at blive overtaget, eller den kan blot sætte sig til at vente og lytte. Enhver med den trojanske hests styreprogram vil herefter kunne få fuldstændig kontrol over computeren, og både starte programmer på den og overvåge, hvad der tastes på tastaturet.

Kombinationer
Der er intet til hinder for, at en orm kan indeholde både en virus, som inficerer dine programmer og sender orm ud i verden, og en trojansk hest, som åbner for styring udefra. Kun virus-programmørernes ubarmhjertige kreativitet sætter grænsen.

Hoax
En hoax er en falsk virusadvarsel, som distribueres via e-mail.

En typisk hoax indeholder en skrækhistorie om en ny virus, som vil ødelægge vitale dele af ens computer, ofte både data og harddisk og skærm. Afsenderen påstår også, at advarslen blev udsendt ”for en uge siden” fra et stort firma som IBM eller Microsoft. Der er dog aldrig et link til en artikel om den farlige virus med, og man kan heller ikke finde noget hos de store antivirus-firmaer om virussen. Beskeden opfordrer altid til, at du hurtigst muligt sender den videre til alle, du kender.

De mere godartede af slagsen har blot samme formål som et kædebrev, hvilket vil sige, at de bare spilder folks tid og belaster mailserverne med unødvendige mails. De mere ondsindede forsøger ikke blot at narre dig til at sende advarslen videre, og få dig til at fremstå som et fjols, men lokker dig også til at slette filer på din harddisk. Den mest kendte hoax, som desværre stadig lever i bedste velgående, er ”jdbgmgr” som forsøger at få dig til at slette filen ”jdbgmgr.exe”, som har en lille bamse som ikon. Filen er en del af Windows, som du kun skal bruge, hvis du programmerer JAVA, men den falske advarsel forsøger altså at bilde dig ind, at den er en virus, som skal slettes.

8 gode råd om sikkerhed

Følg disse enkle råd for at mindske risikoen for at få virus.

Af Stina Christiansen 28/01-2003 (http://sikkerhed.tdconline.dk)

En computervirus er et program, som gør ét eller andet ved din computer, som du helst er fri for og ikke har bedt den om. Ofte er virussen gemt i et andet program eller skjult i en mail. Virus kan resultere i en harmløs besked på din skærm, men det er desværre ofte programmer, som ødelægger filer på harddisken.

En virus vil ofte kopiere sig selv til dine systemfiler, så den er aktiv, hver gang computeren er tændt. Den vil ofte også kopiere sig selv til andre programfiler. Nogle typer spreder sig endda til almindelige dokumenter som for eksempel word-dokumenter og regneark.

1. Tænk dig om

Vær kritisk når du åbner en mail. Hvis det ikke er fra nogen, du kender, eller fra et firma, du selv har kontaktet, så tænk dig om to gange, inden du åbner mailen.

Kig en ekstra gang selvom mailen kommer fra dine venner. Hvis de pludselig skriver til dig på engelsk, eller sender dig en eller anden fil, som I ikke har talt

om, så er der ikke noget forgjort i ikke at åbne mailen eller ringe til dem og spørge, om de virkelig har sendt en mail.

Det er meget let at forfalske afsender-adressen i en mail, og de fleste virusser gør det helt automatisk.

Så et par hurtige spørgsmål: Kender jeg dem, der har sendt mig denne mail - og venter jeg denne fil?

2. Opdater din maskine

Sørg for at holde dine programmer (browser, email-program og operativsystem) opdateret. Leverandørerne kommer jævnligt med opdateringer, der retter fejl og forbedrer programmerne. Opdateringerne er gratis og foregår fra leverandørens site.

Hold øje med nye opdateringer her på sitet og hos Microsoft.

Hvis der ikke automatisk dukker et lille opdateringsikon op på din computer, når Microsoft sender nye opdateringer ud, kan det være fordi din maskine mangler at få opdateret nogle Servicepacks - læs mere om Servicepacks her.

Du kan sætte din computer op til automatisk at hente nye opdateringer. Gå i Start, Indstillinger/Settings, Kontrolpanel/Controlpanel og vælg Automatisk Opdatering/Automatic Updates. Her kan du vælge mellem tre mulighed for at holde din computer nemt opdateret. Har du bredbånd og er på nettet hele tiden, kan din computer selv sørge for at hente opdateringerne og få dem lagt på.

3. Installer antivirusprogram og firewall

Nu om dage kommer du ikke uden om at have et antivirusprogram, der kan scanne de filer, du får ind på computeren og ofte i tide advare om, at filen er inficeret med virus. Programmet kan i mange tilfælde også gå ind og fjerne en virus, hvis du har fået den ind på computeren.
En firewall kan også være en god bremse overfor virus. Den kan fange en orm, der forsøger at komme ind på din computer, hvis den udnytter et endnu ukendt sikkerhedshul.

Er du kunde hos TDC, kan du abonnere på en sikkerhedspakke, som blandt andet indeholder et antivirus-program, som opdateres løbende med beskyttelse mod ny virusser og en personlig firewall.

Sæt dit antivirusprogram til automatisk at kontrollere for virus, hver gang du henter filer - hvor filerne end befinder sig. Husk at opdatere dit virusprogram ofte, da der hele tiden kommer opdateringer på grund af nye virusser.

Du kan se, hvad der sker, når dit antivirusprogram finder en virus, ved at hente en virus-test fil. Filen er IKKE en virus, men den indeholder en kode, som ligner en virus, og som de fleste anti-virus-programmer kan genkende.

Hent virus testfilen ved at klikke på dette link.

Nu skulle dit antivirusprogram gerne reagere ved at komme med en meddelelse om, at du forsøger at hente en fil, som indeholder en virus.

Hvis der ikke sker noget, og du endda kan få lov til at gemme filen på din computer, er der muligvis noget galt med din virus-beskyttelse. Vær dog opmærksom på at filen som sagt ikke er en virus, så muligvis er det blot, fordi testen ikke virker i dit program.

Læs mere om denne test af dit antivirusprogram hos organisationen Eicar.

4. Sikkerhedsniveau i browseren

Du bestemmer selv hvilket sikkerhedsniveau, du vil have i din browser. Vi anbefaler, at du sætter det til Mellem.

Du ændrer det ved at gå op under Funktioner/Tools i din Internet Explorer browser, vælge det nederste punkt Internet indstillinger/Internet Options og derefter fanebladet Sikkerhed/Security. Her trykker du på knappen Standard niveau/Default level og trækker skyderen på siden op eller ned til mellem.

På dette niveau er der en god balance mellem, at du er rimeligt beskyttet, samtidig med at du kan se alle sider på nettet, uden hele tiden at skulle sige ja til browseren, om at det ene og det andet må blive vist. Har du mere forstand på det, kan du vælge dine egne indstillinger.

5. Spam og junkmail

Lad være med at svare på spam og junkmail.

Ja, det er virkelig irriterende, at de har fået fat i din mailadresse. Men det bliver først rigtig slemt, når du skriver til dem, at du er megatræt af alle deres mails eller forsøger at bruge deres link til at afmelde mailen. Så ved afsenderne nemlig, at de har ramt en aktiv adresse, og så bliver din mailadresse først interessant for dem.

Sæt hellere et spamfilter på og undgå mailsene.

Læs hvad du kan gøre mod spam, hvis du er TDC-kunde.

6. Vær kritisk overfor advarsler

Det er helt sikkert de mest velmenende af dine venner, der skynder sig at videresende mails med beskeder om, at den og den fil i virkeligheden er en virus, og at du skal skynde dig at slette den.

Men klap lige hesten, dig selv og computeren, inden du kaster dig ud i at slette noget som helst. Ind i mellem er der desværre flere eksempler på falske beskeder, hvor den fil, der er blevet advaret imod, faktisk skal være på din computer.

Tjek for eksempel et par sikkerhedssites for at se, om der rent faktisk er tale om en virus. Hvis ingen skriver om den, så er der sandsynlighed for at der er tale om en falsk advarsel.

Læs mere om falske og sande advarsler.

7. Undgå uønskede programmer

Indstil din computer til et passende sikkerhedsniveau, så du ikke får installeret programmer, du ikke ønsker, uden at du opdager det (se punkt 4). Vær kritisk før du trykker OK til at installere noget. Hvis et vindue kun har en OK-knap, kan du holde ALT nede og trykke F4 for at lukke vinduet uden videre.

Hvis du vil downloade et program, så læs betingelserne igennem, inden du accepterer downloaden. Vær kritisk med hvad du downloader. Hent det ned på din computer og sørg altid for at viruschecke det, inden du pakker det ud på din maskine.

8. Passwords

Sørg for med jævne mellemrum at skifte dine passwords. Vær lidt snu, når du udtænker dem - lad være med at bruge dit eget navn, dit telefonnummer eller fødselsdato. Man skal ikke ret langt ind på livet af dig for at være i stand til at gætte det.

Så vær kreativ og skift passwords ofte.