Virus

1 Målgrupp

Alla datorer som är uppkopplade på Umeå universitets datornät ska ha ett fullvärdigt skydd mot virus. Datorer som ej uppfyller detta krav kan komma att kopplas bort från nätet.

2 Allmänt

Syftet med detta dokument är att beskriva hur man som anställd ska skydda sin dator mot angrepp som virus, trojaner och maskar, d.v.s. alla typer av malware.

Ett virus är ett oönskat program som har som syfte att kopiera sig själv och på så sätt smitta andra datorer. Virusets syfte är ofta både att sprida sig så fort och till så många som möjligt men kan ofta också ställa till stor skada. Ett virusprogram kan ofta få fäste på en dator p.g.a. felaktigheter i operativsystem eller programvara som inte har åtgärdats.

Flera kända virus använder sig av din adressbok och sparade webbsidor (internet-cache) för att hitta nya adresser att skicka sig vidare till. Mottagaren kan sättas till slumpmässig mottagare (dvs. den som den just då råkade hitta någonstans på din dator) och även slumpmässig avsändare. För att verkligen ta reda på varifrån det ursprungliga viruset skickats måste man analysera brevhuvudet. Det finns också virus som skickar dokument vidare som fanns på den infekterade datorn. På detta sätts sprids både affärshemliga och personliga dokument till sådana som finns i den aktuella adressboken.

Datavirus kan komma in i datorsystemen via många olika vägar. Ofta är det i form av lagrade program eller bilagor till e-post eller andra meddelandeprogram (som exempelvis MSN). Men även spridning via nätverket kan förekomma (då kallas de ofta maskar). Virus kan också komma i form av bilagor till e-post eller makron som används i exempelvis ordbehandlingsprogram. Ett sätt som viruset sprider sig på är att gömma sig tillsammans med andra program eller filer. Många virus maskerar sig genom en text som inbjuder till att du ska öppna den bifogade filen: Den erbjuder sig vara allt ifrån en häftig skärmsläckare till en ny fix för Windows. Ofta tillsammans med en text som anger något i stil om att "Microsoft har just släppt denna fix och vill absolut att du ska installera den omedelbart!"

För virus där både avsändare och mottagare sätts slumpmässigt kan du komma att få meddelande om att du har skickat virus. Det som händer är att mottagarens e-postserver har ett inbyggt filter mot virus. Filtret konstaterar att ett virus har mottagits och returnerar ett meddelande om att brevet är infekterat till den som den tror är avsändaren - i det här fallet du själv. Får man ett sådan här meddelande om att man skickat virus ska man dock inte direkt avfärda det som ett falskt alarm utan verifiera att man själv verkligen inte har virus.

Idag förekommer ofta blandade attacker: D.v.s. det vi traditionellt tidigare har kallat för virus kan idag innehålla komponenter som såväl skickar skräppost via den egna datorn, söker efter andra datorer att infektera samtidigt som det öppnar en bakdörr och ge hackaren access och

kontroll över datorn.

3 Policy

Alla datorer som är anslutna till Umeå universitets datornät måste ha ett tillräckligt virusskydd. Alla användare av Umeå universitets datornät ska i sin hantering av dokument och applikationer uppträda på ett sådant sätt att möjlighet till virusinfektering undviks. Installerad antivirusprogramvara ska uppdateras regelbundet, både vad det gäller programversion och antivirusdefinitioner.

Iaktta försiktighet med bifogade filer som skickas till dig via e-post eller annat medium. Öppna inte bifogade filer som du inte förväntat dig att få eller som du inte på annat sätt kan verifiera att de inte innehåller virus, t.ex. genom att antivirusprogrammet har kontrollerat filen först. Se dock till att ditt antivirusprogram är uppdaterat innan du öppnar ett brev som du känner dig osäker på.

Eftersom vissa virus sprids via säkerhetshål i operativsystem eller applikationsprogram är det viktigt att installera viktiga säkerhetsuppdateringar för operativsystem och installerade applikationer.

Det är vanligt att det via e-post sprids falska virusvarningar. Du ska aldrig skicka dessa vidare! Falska virusvarningar tar tid att hantera, och leder till att du och dina kollegor förr eller senare inte tar äkta varningar på allvar. Om du får en virusvarning i din brevlåda, kontakta IRT (irt@umu.se) eller Service Desk vid ITS för att kontrollera om den är relevant eller inte.

4 Regler

Acceptera aldrig filer om du inte är 100 % säker på innehållet. Det spelar ingen roll om avsändaren är känd eller inte, då flera virus sätter en godtycklig avsändare och/eller mottagare.

Öppna heller aldrig bilagor som du inte väntat dig att få i din brevlåda. Det gäller oavsett om brevet är skrivet på svenska eller engelska, och oavsett om du känner avsändaren eller inte.

<u>Om misstanke finns om att en dator är virusinfekterad:</u>

Dra ur nätverkssladden. Många virus sprider sig via e-post; genom att dra ur nätverkssladden kan du förhoppningsvis hindra viss spridning.

Stäng inte av datorn. Detta är dels för att man vid felsökning ska kunna se vilka program är igång på datorn, och dels för att vissa virus är programmerade att utföra kommandon vid omstart.

Försök att med hjälp av ditt antivirusprogram rensa datorn från virus. Se då till att ha uppdaterat till den senaste versionen av antivirusprogrammet för att öka chanserna att rensningen lyckas. Hämta aktuella antivirusfiler från tillverkaren.

Scanna datorn med ditt antivirusprogram och följ anvisningarna. Se också instruktionerna på antivirustillverkarens hemsida, eftersom borttagning av vissa mer besvärliga virus kräver mer

än bara körning av antivirusprogrammet.

Om inget virus hittades: Kontrollera att själva antivirusprogrammet är den senaste versionen om så inte är fallet: Uppdatera antivirusprogrammet och gör om scanningen.

När datorn är rensad från virus ska ytterligare en scanning köras för att förvissa sig om att inga eventuella virus finns kvar.

Om fortfarande inget virus hittas, trots uppenbara indikationer om detta: Kontakta Service Desk på ITS för assistans.

5 Definitioner

Trojansk häst/Trojan: Ett program med dolda destruktiva funktioner.

Virus: Ett dataprogram som sprider sig själv genom att lägga till sig på andra objekt.

Mask: Ett dataprogram som oberoende replikeras genom att skicka sig själv till andra datorer.

Hoax: Ett kedjebrev som vanligtvis handlar om en falsk virusvarning.

Skämtprogram/Joke: Ett program med störande eller roliga funktioner, men ej destruktivt.

Malware: Ett vanligt namn för alla typer av oönskade mjukvaruprogram såsom virus, maskar, trojaner och skämt.

Scanna: Avsökning av t.ex. innehållet på en hårddisk eller tillgängliga tjänster på en dator

6 Se också

7 Revisionshistoria

Fastställt 2011-03-21/ Maria Tauson