

# Information om datasäkerhet och brandväggar för oss inom Akalla Husby Nätort

Denna sida är till för att informera OSS ALLA hur vi kan skydda oss när vi är ute och surfar på Internet eller laddar hem e-post. Problemet med skadlig kod, eller det vi vanligen kallar virus, är att det inte BARA drabbar oss själva, UTAN OCKSÅ förstör trafiken och åtkomsten för våra grannar inom AHN.

När en dator blir smittad kan den börja ”pumpa ut” 100.000-tals små meddelande per timme som gör att andra användare på AHNs nät inte kommer ut på Internet. Det räcker alltså med 1 stycken smittad dator för att förstöra för alla andra medsurfare i AHNs nät. Detta har ni redan säkert känt av stundtals, då det känns som att ni inte kommer någonstans när ni är ute och surfar. Ofta kommer ni upp i den ”otroliga” hastigheten av 0,01 kb/s. Vem som orsakar den proppen på vårt AHN-nät kan nämligen väldigt lätt spåras och spåras de facto upp. Inte vill väl du vara den som orsakar problem för alla dina grannar?

Här kommer 3 enkla råd hur du bäst undviker att själv bli smittad och att smitta andra:

1. Använd en brandvägg ut mot Internet. Det kan vara en mjukvarubrandvägg eller en separat liten hårdvarubrandvägg. De som använder router har OFTAST en inbyggd brandväggfunktion. Att använda Internet UTAN brandväggsskydd är som att INTE låsa ytterdörren när man går hemifrån på morgonen. Det är lika självklart att använda ett brandväggsskydd när man är ute på Internet som att låsa ytterdörren när man lämnar hemmet och ingen finns kvar hemma att vakta mot inkräktare. UTAN brandväggsskydd är du helt utlämnad till att vilken kunnig person som helst kan ta sig obemärkt in i din dator och snoka omkring och stjäla koder, lösenord och ibland även din identitet (IP-adress). Om sedan ett brott begås så är det dina fingeravtryck som kommer att synas.
2. Se till att ha AUTOMATISKA UPPDATERINGAR påslaget till ditt operativsystem. Över 90% av alla hemanvändare använder sig av något av Microsoft's operativsystem. Se till att aktivera ”automatiska uppdateringar”. I dessa uppdateringar följer det med s.k. ”fixar” eller ”patchar” som kan liknas vid ”tätningsgummi” som tätar de säkerhetshål som man efterhand upptäcker i operativsystemet (OS). Exempelvis kan du aktivera automatiska uppdateringar i Windows XP genom att trycka på ”Start”-knappen, välja Kontrollpanelen och i den trycka på ”säkerhetscenter”. I ”säkerhetscenter” kan du koppla på ”automatiska uppdateringar”. Ett annat sätt, lite mer tillfälligt, är att i Internet Explorer, under menyn ”verktyg” välja ”windows uppdater”. Då kopplas du automatiskt till Microsofts sida för senaste uppdateringarna.
3. Ha ALLTID ett BRA och dagligen uppdaterat antivirusprogram och se till att permanetskyddet ALLTID är påkopplat när du är i kontakt med Internet på något sätt. Det finns flera bra antivirusprogram som har brandvägg integrerat i sig. Välj dessa. Den gamla regeln: ”Du får vad du betalar för” gäller även här. Visst kan du ha något gratis-antivirusprogram, men tillförlitligheten blir tyvärr ofta därefter. Med andra ord,

du köper antagligen inte ett ytterlås till din dörr där hemma för 1 krona, varför skulle du då med samma logik, förlita dig till ett gratis antivirusprogram? Exempel på bra antivirusprogram är Norton, McAfee och Panda. Vänd dig till Rune Pettersson, Brf Husby Nr 1, som genom ett avtal mellan AHN och pandas svenska generalagent kan sälja Panda antivirus till AHN-an slutna till reducerat pris mot vad du får betala i handeln.

Mer information om vilka virus som är mest aktiva för stunden kan du få på:

[http://www.pandasoftware.com/virus\\_info/](http://www.pandasoftware.com/virus_info/)

Andra råd och tips kan du få här:

<http://www.microsoft.com/athome/security/protect/default.aspx>

Nedan följer en liten "ordlista" för alla de skadliga elakheter som huvudsakligen sprids via Internet:

Malware (Malicious Software) elakartade program: (**Fetmarkerade** är de som vanligen omfattas av begreppet "virus")

**Virus – Skadlig kod**

**Trojaner – kod som tar sig in obemärkt och exekverar sig när du trycker på det eller det är "på plats"**

**Maskar – skadlig kod som delar sig/sprider sig mycket snabbt genom delning. (Exvis loveletter)**

Spyware – Skickar ut information till andra från din dator (Exvis Gator, spårande cookies, Ist bar)

Hacker Tools – Verktyg som gör att en obehörig kan ta över datorn och "göra vad de vill med den". (Exvis, Net Bus, Portscanner, Superscanner, Win Nuke)

Skämtvirus – Skämtprogram (Exvis Full mus, "Nu formateras din hårddisk")

Säkerhetsrisker (vulnerabilities) – Om man saknar en viss "patch" kan detta användas för att ta sig in i din dator eller skapa problem att exvis köra Internet Explorer. (Exvis använde sig Blaster-viruset av denna säkerhetsrisk)

Hoax – man uppmansa och luras att ta bort en fil (som sägs vara infekterad) som man ABSOLUT INTE skall tas bort (Exvis jdbgmgr.exe, Macrovirus som drabbar Microsoft)

Spam – oönskad och ibland smittad e-post.

Phishing – meddelande som ses som trovärdiga (från en bank eller liknande) vilka lurar dig att uppge vissa personliga koder och sänder dessa till en helt annan URL/adress (Citibank, Eurocard etc) se gärna: [www.antiphishing.org](http://www.antiphishing.org) för info om de senaste bedrägerierna.

Spoofing - "Kidnappning" av en (kan vara din) identitet eller användarkonto, där kidnapparen använder sig av din IP-adress som täckmantel för att begå brott.

Ovan beskrivna "verktyg" kan enkelt användas för att åstadkomma DDOS (Distributed Denial Of Service) eller DOS (Denial Of Service)-attacker. Det är när dessa pågår som du upplever att det går väldigt långsamt att ta sig ut på Internet. Tyvärr är det då ofta någon av dina intet ont anande och oskyddade grannar i AHN, som med otillräckligt datorskydd har kopplat upp sig mot Internet och bokstavligen "sprutar ut" smittad trafik, som tränger ut dig från att komma ut på Internet. DOS är alltså VERKAN av att någon medvetet eller omedvetet, använder dessa "malware" för att "bomba" en server eller en sajt etc – inte ett "malware" i sig. Tyvärr pekar trenden mot ytterligare nya och kombinerade former av malware för att åstadkomma DOS. Till detta kan läggas en kraftig utökning av dagens moderna "löss" – SPAM.

Så för din och allas vår trevnad i AHN– skydda din dator på bästa tänkbara sätt!!!

Alexander Boksjö  
Brf Husby 1