



# *SurfaLungt*



Säkerhet på Internet

Sammanställt av Bengt-Göran Carlzon

# Säkerhet på Internet

Bristande säkerhet på Internet beror i första hand på 3 saker

1. Okunskap
2. Slarv
3. Oseriösa användare

## Informationssäkerhet

För mycket skydd gör informationen värdelös. "Ingen" kommer åt den.

För lite skydd gör informationen osäker.

Informationssäkerhet är inte en produkt-  
Det är en attityd som tar hjälp av produkter.

## Vilka är hoten?

- Skräppost ( spam )
- Virus, spionprogram ( spyware ) mm
- Överbelastningsattacker
- Lagring av olagligt material
- Sniffa knapptryckningar
- Avlyssna datatrafik
- Identitetsstöld
- Plus ett antal saker till...



Zombie = kapad dator

Botnet = en samling ( nätverk ) av kapade datorer

## Spamming = spridning av skräppost

- Mer än 60% av all spam skickas ut via kapade hemdatorer.
- I 99% av fallen är ägaren fullkomligt omedveten om vad som sker via hans dator.
- Att spamma via BotNets är ett relativt säkert sätt för förövarna att undvika att bli spårade.
- Majoriteten av alla bedrägeriförsök (phishing, Nigeriabrev o dyl.), reklam för barnpornografi mm skickas därför via kapade hemdatorer.
- En kapad hemdator ansluten till bredband kan skicka ut 100,000 tals spam per dygn.

## **Överbelastningsattacker**

- Används i utpressningssyften, på beställning av en konkurrent eller i rent sabotagesyfte.
- Även ett BotNet med 1000 zombies kan orsaka stor skada. Om genomsnittsbåndbredden är ~ 1 Mbits/s så har dessa tillsammans en gemensam eldkraft på 1 Gbits/s.
- En BotNet-attack är mycket svår att stoppa eftersom attacken kommer från en massa olika håll samtidigt.

## **Lagring av olagligt material**

- En kapad dator kan användas som lagringsplats för olagligt material.
- Den kan även agera som en webbserver för samma ändamål. Populärt för att lagra falska bankwebbsidor och andra sidor där förövaren vill lura till sig personlig eller finansiell information. Det finns exempel på olagliga sajter där den publika webbservern själv inte innehåller några filer utan dessa finns länkade vidare ut på ett antal kapade hemdatorer.

## **Identitetsstöld**

- BoNets används för storskalig identitetsstöld vilket är ett av de snabbast växande problemen på Internet. Hit räknas Phishing, kreditkortsnummer, personlig information mm

## **Zombie = kapad dator**

- En zombie är en dator som smittats utav elak kod som gör att en utomstående kan ta full kontroll över datorn. Även kallad "kapad dator"
- Man kan smittas via infekterad e-post, via en webbsida eller direkt dator-till-dator.
- En oskyddad dator kan smittas på ca 30 sekunder.
- I dag räknar man med att det finns ca 90,000 zombiedatorer i Sverige – i världen troligtvis miljontals.
- Antalet zombies ökar i snitt med ca 300st om dygnet.

### **BotNet = en samling kapade datorer**

- Ett BotNet är ett antal zombiedatorer som ingår i ett och samma nätverk.
- Ett BotNet kan bestå av 100-tals upp till 100,000 zombies.
- Antal BotNets i världen är okänt.
- BotNets köps, säljs och uthyres som vilken annan vara som helst.
- Ju snabbare förbindelse som zombien sitter på, desto högre värde.

### **Sverige är inte säkert!**

- 89% av svenska folket använder Internet
- 35 % av användarna har inte antivirusprogram
- 20 % av mindre företag har inget eget virussydd
- 67% av svenska företag infekterades minst en gång
- Få hemanvändare nyttjar en personlig brandvägg
- 54 % av mindre företag har egen brandvägg
- I snitt blir alla användare smittad varje år

### **Enkla åtgärder**

- Din dator är ditt arbetsredskap  
Låt ingen annan använda den (och om du gör det –ha separata lösenordsskyddade konton)
- Sätt upp en säkerhetspolicy / regler  
Även om ni inte är så många är det viktigt att klargöra vilka regler som gäller, samt vad som händer vid en incident (krisplan), och vad som händer om man bryter mot en regel
- Stäng av alla funktioner och tjänster som du inte använder
- Kom ihåg att regelbundet uppdatera operativsystem och övrig programvara



### **Hur vanligt är det att råka ut för en incident?**

- "27 procent av svenska företag med upp till 100 användare har någon gång förlorat information eller haft driftstopp på grund av intrång eller virusangrepp"
- "I 68 procent av fallen ledde detta till att systemen låg nere, i största delen av fallen mer än 8 timmar" ...alltså mer än en arbetsdag
- Ändå uppger 37 procent att de har god eller mycket god kontroll över IT-säkerheten

### **Surfa Lugnt!**

- En nationell kampanj för att öka medvetenheten om vikten av ansvar på nätet
  - För sig själv
  - Och därmed för andra ( [www.surfalungt.se](http://www.surfalungt.se) )
- 15 organisationer/myndigheter/företag som samverkar
- Ett antal lokala/regionala kampanjer, sammanhållna av en "kampanjgeneral"
  - Bygger på lokalt engagemang
- Målgrupper: småföretag, tonåringar, hushåll

### **Varför en kampanj?**

- Omedvetenhet om att man skadar andra om man inte skyddar sig
- Inom 60 minuter har en ny PC på nätet utsatts för 4-6 intrångsförsök

### **Åtta goda råd**

1. Ha uppdaterad brandvägg och antivirusprogram.
2. Uppdatera operativsystem och webbläsare regelbundet.
3. Ta kopior regelbundet.
4. Var noga med lösenord.
5. Var försiktig med personliga uppgifter.
6. Undvik skräppost –använd flera e-postadresser.
7. Var vaksam på bifogade och nerladdade filer.
8. Kontrollera regelbundet datorn.

