# Ormehuller i internettet som kur mod orme

**Forskere forslår at opbygge et netværk af særlige lokkemaskiner, som kan opspore nye orme og sprede vaccinen mod dem gennem særlige genveje i internettet.**

- Af Jesper Stein Sandal
- Offentliggjort fredag 2.december 2005 kl. 15.04

Et netværk af lokkemaskiner med adgang til særlige smutveje på internettet kan måske fungere som værn mod internetorme, viser israelske forskeres simuleringer.

I det videnskabelige tidsskrift Nature Physics præsenterer forskerne derfor en mulig opskrift på en kur mod orme, der spreder sig via internettet.

**Netværk skal gøres immunt**

- Vores fokus har været at gøre hele netværket immunt, ikke at rense hver enkelt pc eller reparere noget, efter det er gået i stykker, siger professor Eran Shir fra Tel Aviv University til Nature.com.

Opskriften, som Eran Shir og hans kolleger foreslår, går ud på at oprette et netværk af lokkemaskiner, også kaldet "honeypots".

Disse maskiner kan opfange internetorme og generere et digitalt fingeraftryk, som andre pc'er kan bruge til at identificere og afvise ormene.

Den proces er ikke anderledes, end den måde antivirusfirmaerne allerede bekæmper orme på.

**Forbindes med beskyttede veje**

Eran Shirs forslag går derfor på, at man forbinder disse lokkemaskiner med beskyttede genveje på internettet.

Det vil sige, at "vaccinen" mod en ny orm kan spredes via en genvej og nå frem til slutbrugerne, før ormen gør det.

Det skal løse det problem, som i dag plager antivirusfirmaerne, nemlig distributionen af deres opdateringer.

I visse tilfælde kan der gå flere dage, før alle slutbrugere har modtaget det nødvendige fingeraftryk, som gør deres antivirusprogram i stand til at beskytte dem.

Ifølge de israelske forskeres simuleringer af, hvordan et sådant netværk af lokkemaskiner og "ormehuller" i internettet vil fungere, skal netværket blot bestå af 0,4 procent lokkemaskiner placeret på strategisk rigtige steder.

Selvom det ikke lyder af meget, så vil det alene i USA betyde, at der skal opstilles 800.000 af disse maskiner.

**Teknologien findes**

Til gengæld vil det betyde, at ud af de 200 millioner pc'er i USA, vil blot 2.000 blive inficeret.

Teknologien til at overvåge netværket og spore trusler findes allerede i form af forskellige intrusion detection-systemer.

Selv om man også har en god idé om, hvor det vil være strategisk klogt at opstille lokkemaskinerne, så er den israelske idé ikke skudsikker, mener andre eksperter.

- De her virusprogrammører er ikke dumme, og de kunne derfor finde en måde at angribe selve det parallelle netværk, advarer professor i informatik Alessandro Vespigiani fra Indiana University over for Nature.com.

De israelske forskere har ingen planer om at bygge et kommercielt produkt på baggrund af deres antivirus-model.

I stedet vil de forsøge at opbygge et open source-projekt, som internetbrugere frivilligt vil kunne tage del i, skriver Nature.com.