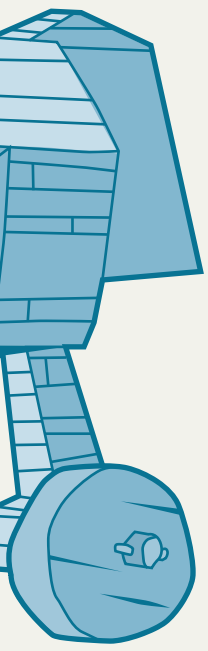
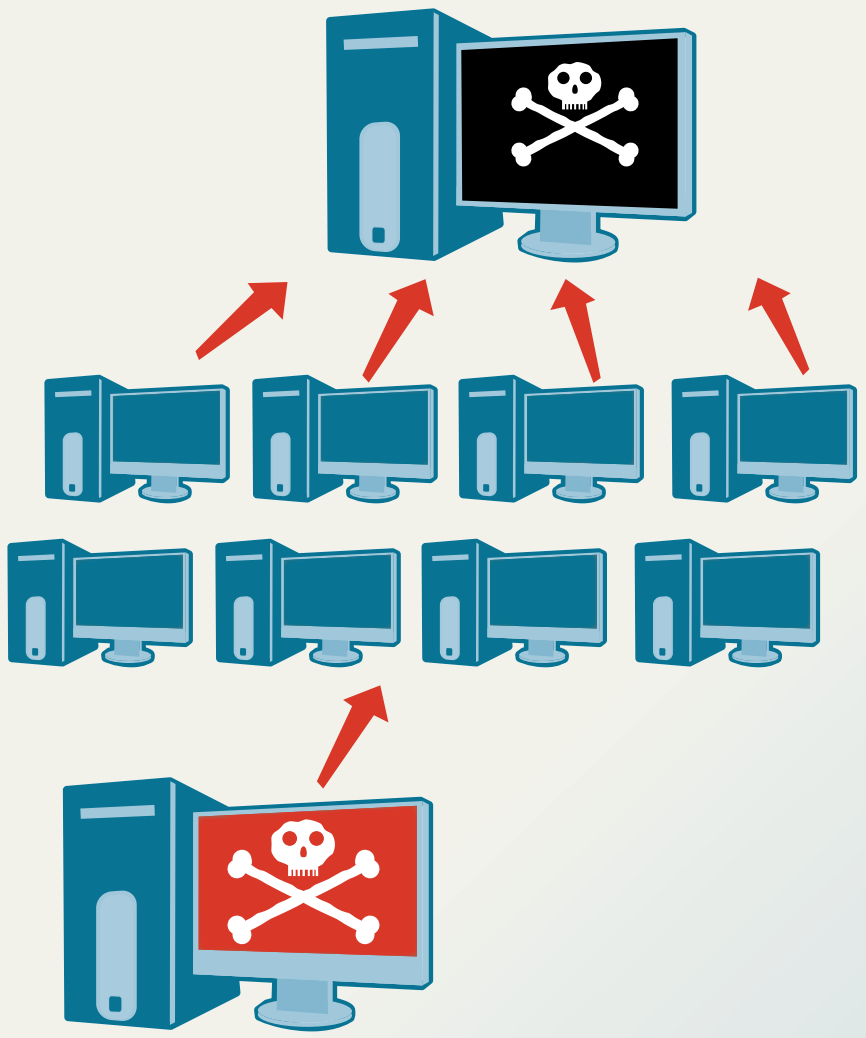


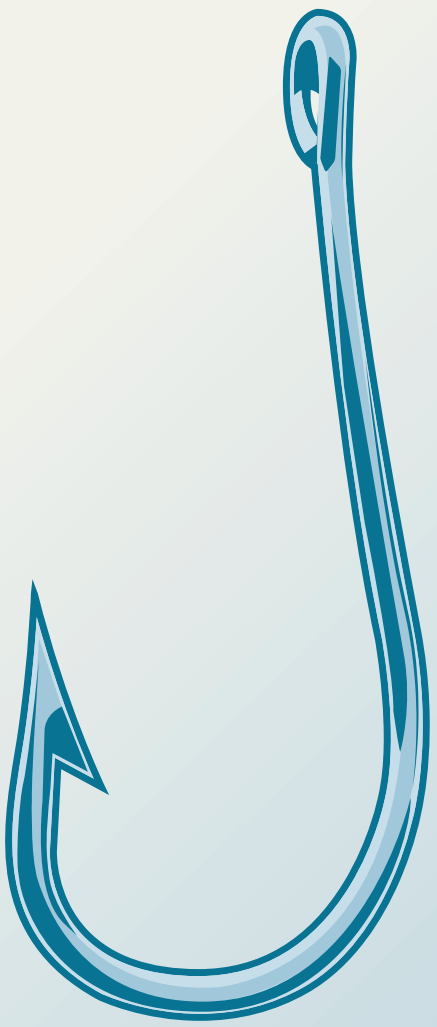


DDoS-angreb

DDoS står for *Distributed Denial of Service* (distribueret servicenægtelse), og er betegnelsen for et angreb der bevidst overbelaster en internetserver i en sådan grad at reelle forespørgsler til serveren ikke kan besvares i tide.

Til dette formål bruges et program som er spredt til adskillige andre maskiner på nettet, hvor de alle på én gang i én uendelighed forespørger den samme internetadresse.

Da bedriften er et decideret angreb, kalder man det et DDoS-angreb.



Phishing

Phishing er et internetfænomen, hvor svindlere forsøger at franarre godtroende internetbrugere deres brugernavn, adgangskode, kreditkort- eller netbankoplysninger.

Det sker typisk ved at brugeren får tilsendt en e-mail eller fx en direkte besked på Twitter, hvis indhold forsøger at få brugeren til at indsende sine oplysninger pr. e-mail eller logge ind på en falsk internetside, der ligner f.eks. bankens.

Mailen kan fremstå, som om den er afsendt fra et socialt medie, en auktionshjemmeside, en IT administrator eller en person fra modtagerens adressekartotek.

Din værste fjende er i voldsom vækst

HAR DIN VIRKSOMHED styr på IT-sikkerheden? Tal viser, at flere og flere virksomheder angribes af hackere, men langt fra alle er bevidste om problemet

TEKST: **KLAUS KNAKKERGAARD**
klkn@fynskemedier.dk

Det drejer sig om minutter.

Mere skal en dygtig hacker ikke bruge, så kan han forvandle din blomstrende virksomhed til en overlevelse for konkurs.

Erhvervsavisen Fyn sætter i denne udgave fokus på IT-sikkerheden, og billedet er skræmmende: Det har aldrig været lettere at hacke. Antallet af angreb er voldsomt stigede. Og det er langt fra alle virksomheder, der bekymrer sig om problemet.

Palle Bonnavill er business development manager hos IT-sikkerhedsfirmaet Fortconsult. Hans tal underbygger det triste billede.

- Sidste år så vi en stigning på langt over 300 procent af det, vi kalder DDoS-agreb. Så jo, det er absolut noget, vi kan se en stigning i, fortæller han.

Ved et DDoS-angreb sender hackeren så stor en mængde data af sted mod en hjemmeside, at den til sidst lægges ned. Det er et forholdsvist let og billigt angreb at sætte i værk. Til gengæld kan følgerne være katastrofale.

- Forestil dig, at du har et rejsebureau, hvor folk booker rejserne online. Hvis din hjemmeside lægges ned, så er kan det være mange millioner, du mister i indtjening, fordi du i en periode ikke er online og tilgængelig på nettet, fortæller Stinne Ølshøj fra Dahlberg empowered by Söderberg & Partners, der blandt andet mægler forsikringer mod cyber-kriminalitet.

Få nu gjort noget

Det er umuligt at fastslå det præcise antal hackerangreb mod virksomheder i Danmark. En stor del anmeldes ikke, og endnu færre offentliggøres andre steder, da det sjældent er en styrkelse af et image at blive hacket.

En undersøgelse fra revisionssammenslutningen KMPG giver dog en fornemmelse af, hvor meget problemet vækster.

Den viser blandt andet, at ud af de samlede registrerede hackerangreb i 2012 var 52 procent rettet mod virksomheder. I 2010 var tallet blot otte procent.

Men der findes også positive tendenser.

- Det er heldigvis begyndt at blive et emne, som ikke længere kun er på it-chef niveau. I de virksomheder, der tager problemet alvorligt, er det i højere grad på ledelsesniveau. Og det er et vigtigt sted at begynde, så it-chefen ikke hele tiden skal argumentere for, at det er vigtigt, siger Palle Bonnavill.

Og selv om det umiddelbart kan lyde dyrt for en mindre virksomhed at beskytte sig mod it-kriminalitet, så bør man hellere gøre lidt end intet.

- Bid indsatsen over på tre år. Vi anbefaler, at man så det første får lavet et tjek af en tilfældig arbejdslaptop.

Hvad kan kriminelle få ud af den, hvis medarbejderen glemmer den i lufthavnen eller får den stjålet. Det giver et ret godt billede af sikkerheden, forklarer Peter Bonnavill.

Og ligesom alle andre eksperter peger han på den sunde fornuft som en af de vigtigste værn.

- Du skal sørge for en sund kultur i virksomheden. Vi testede en stor dansk virksomhed ved at sende en mail ud, hvor vi skrev, at medarbejderne være med i lodtrækningen om en bil, hvis de bare indtastede deres brugernavn og password. Det er det, vi kalder "phishing". 25 procent af medarbejderne indtastede deres oplysninger. Havde vi haft onde hensigter, havde de lige gjort vores job meget lettere.

- Hackerne bliver bedre hele tiden, og det gør sikkerhedssystemerne også, men det hjælper ikke så meget, hvis man ikke husker at bruge fornuften.