

## ISP Sikkerhedsforum

- *De danske internetudbyderes frivillige samarbejde for sikkerhed på internettet*

# Adfærdskodeks om nedbringelse af spam



## Adfærdskodeks om nedbringelse af spam

### Baggrund

Medlemmerne af ISP-Sikkerhedsforum blev i efteråret 2004 enige om at undersøge mulighederne for at nedbringe mængden af spam på internettet, med henblik på en konkret indsats på området.

ISP-Sikkerhedsforum har løbende været i kontakt med Videnskabsministeriet og har blandt andet i forbindelse med vurderingen af konkrete spam-bekæmpende tiltag taget udgangspunkt i rapporten: "*Oversigt over teknologiske løsninger, der kan bidrage til at minimere/fjerne spam*", der blev udarbejdet over sommeren 2004 som led i møderækken vedr. spam i Videnskabsministeriet.

De danske internetudbydere gør samlet set allerede i dag en målrettet indsats på området, og denne kodeks tager derfor udgangspunkt i at beskrive og kodificere en række af de allerede eksisterende arbejdsgange.

### Afgrænsning

Denne kodeks tilsigter at nedbringe mængden af spam afsendt fra eller modtaget hos private danske brugere af internettet.

Grundlæggende er spam en samlebetegnelse for e-mails, som sendes uanmodet, og som dermed set fra modtagerens side er uønskede. For afsenderen af spam vil der typisk være tale om en enslydende forsendelse afsendt til en større mængde email-adresser. Spam er typisk uvedkommende for modtageren, i betydningen:

- At modtageren ikke har bedt om den.
- At indholdet ikke umiddelbart er relevant for modtageren.
- At modtageren ikke er direkte relateret til indhold eller afsender.
- At der er tale om en "rundskrivelse", som er kommunikeret til modtageren elektronisk.
- At afsenderen typisk har forsøgt at skjule sin identitet.

Denne kodeks behandler alene forhold, der vedrører nedbringelsen af afsendte spam-mails fra danske internetbrugere, samt nedbringelsen af mængden af modtagne spam-mails hos danske internetbrugere. Kodeksen omfatter ikke forpligtelser i forhold til e-mails sendt fra og modtaget af erhvervsvirksomheder. Dette skyldes, at mange professionelle brugere af internettet selv ønsker at forestå den nødvendige filtrering heraf.

### Indsatsen

I forbindelse med udarbejdelsen af kodeksen har det vist sig ikke at være muligt at implementere ensartede tekniske tiltag på tværs af samtlige ISP'ere. Dette skyldes dels at man arbejder på forskellige teknologiske platforme, at der er forskelle på de

individuelle udbyderes netværks art og anvendelse samt at udbyderne har forskellige produktporteføljer, som vil kræve differentiering af de konkrete tekniske tiltag overfor spam.

Det skal i denne sammenhæng understreges, at kodeksens første punkt - forpligtelsen om at tilbyde kunderne centralt baserede intelligente filterløsninger – forventelig vil reducere antallet af modtagne spam-mails hos danske internetbrugere markant. Det forventes i forlængelse heraf, at effekten af yderligere tekniske tiltag alene vil kunne nedbringe mængden i begrænset omfang, da visse af disse tiltag primært er afhængige af, at tilsvarende foranstaltninger implementeres bredt på international plan for at kunne opnå den optimale præventive effekt heraf.

Endelig må det konstateres, at selve værktøjerne til bekæmpelse af spam vil ændre sig og udvikle sig over tid. Derfor opstiller kodeksen klare mål for indsatsen, mens de mere konkrete midler til målenes opnåelse bør levne rum for såvel individuel tilpasning som almindelig teknologisk udvikling.

### ***Adfærdskodeks***

- **Centrale filtre**  
ISP'erne forpligter sig til at implementere eller tilbyde intelligente, centralt baserede filter-løsninger til nedbringelse af indgående spam, der passerer via ISP'ernes mail-servere.
- ISP'erne forpligter sig til på de respektive selskabers hjemmesider at oplyse om karakteren af det centrale filter, som selskabet tilbyder, herunder eksempelvis om:
  - filteret er fast
  - filteret er slået til som standard
  - der er opt-in/opt-out-mulighed
  - der er flere niveauer for aktivering af filteret (eks: lav, middel, høj)
- ISP'erne forpligter sig til på de respektive selskabers hjemmesider tydeligt at henvise til relevante steder på internettet, hvor den enkelte bruger kan finde information om hvorledes man kan sikre sig mod spam, f.eks. [www.it-borger.dk](http://www.it-borger.dk)
- ISP'erne forpligter sig til at sikre, at deres abonnementsvilkår er udformet, så det er muligt at reagere overfor kunder, der udsender spam. Det skal således fremgå af abonnementsvilkårene, at udsendelse af spam anses for en misligholdelse af abonnementsaftalen, og at en sådan adfærd kan medføre modforanstaltninger som f.eks. lukning af forbindelsen og opsigelse af abonnementsaftalen.
- ISP'erne forpligter sig til at sikre, at der kan videregives oplysninger til dem om uønsket adfærd i form af afsendelse eller modtagelse af spam samt til at sikre, at

udbydere har indrettet deres organisationer således, at henvendelser om spam behandles samt at relevante myndigheder inddrages om nødvendigt.

En anmeldelse om afsendelse eller modtagelse af spam skal kunne foretages enten via e-mail eller pr. brev.

- ISP'erne forpligter sig til at etablere et kontaktnetværk til håndtering af spamsager. Dette kan ske indenfor rammerne af det eksisterende samarbejde i ISP-Sikkerhedsforum.
- ISP'erne forpligter sig til at sikre, at der er udarbejdet konkrete instrukser til medarbejderne om, hvordan de skal behandle forskellige typer af uønsket adfærd vedrørende afsendelse eller modtagelse af spam blandt deres kunder.
- ISP'erne forpligter sig til løbende at følge udviklingen på spam-området, herunder deltage i ISP-Sikkerhedsforums arbejde herom. Internationale erfaringer på området inddrages i dette arbejde.
  - ISP'erne forpligter sig herunder til at følge udviklingen inden for teknologier til bekæmpelse af spoofing af maildomæner, f.eks. Sender-id, SPF eller DomainKeys samt til at støtte op om den teknologi, der på sigt vinder udbredelse.
- Det anbefales, at ISP'erne generelt forhindrer direkte adgang fra kunderne mod omverdenen via port 25, i den udstrækning det er muligt for den individuelle udbyder i forhold til teknologiske eller produktmæssige hensyn.
  - Det anbefales herunder, at ISP'erne i særdeleshed forhindrer adgang fra kunderne mod omverdenen via port 25, hvor kunden måtte have dynamisk IP-adresse.
- **Relay services**  
ISP'erne forpligter sig til at sikre, at anonyme relay services kun kan anvendes fra eget net.  
I det omfang det er muligt for den individuelle udbyder ud fra teknologiske eller produktmæssige hensyn anbefales følgende:
  - at ISP'erne anvender "rate limiting" i forbindelse med anonyme relay services for at begrænse mængden af spam, der kan udsendes fra en kompromitteret kunde.
  - at ISP'erne tilbyder kunder AuthSMTP baserede relay services.

Denne kodeks er gældende fra 1. august 2005, og revideres én gang årligt.

De tiltrådte selskaber forpligter sig til senest pr. 1. januar 2006 at efterleve de forpligtelser, der er anført i denne kodeks.

---

For TDC A/S

---

For DK-Cert

---

For Telia A/S

---

For Webpartner A/S

---

For Sonofon A/S

---

For Tele 2 A/S

---

For Cybercity A/S

---

For Dansk Bredbånd A/S

---

For A+ A/S