

Antispamvejledningen

I lyset af de stadig større mængder spam, vi alle oplever, og i lyset af de ændringer af markedsføringsloven, som blev gennemført i sommeren 2003, har ITEK og DI's it-sikkerhedsudvalg besluttet at forfatte denne vejledning om, hvordan man kan undgå spam.

I vejledningen defineres det, hvad spam er, og det belyses, hvor stort et omfang problemet har. Herefter gives der nogle gode råd til, hvordan man teknisk og ved at anvende e-mails på en hensigtsmæssig måde kan begrænset problemets omfang. Endelig redegøres der afslutningsvist for, hvad markedsføringslovens bestemmelser om spam går ud på således, at virksomhederne ikke kommer i en situation, hvor deres eget reklamemateriale kan betragtes som spam.

Målgruppen for denne vejledning er alle, der ønsker at undgå spam. Privatpersoner kan få nogle gode råd til, hvordan de gennem en hensigtsmæssig anvendelse af e-mails kan reducere sandsynligheden for at modtage spam. Virksomhederne kan få nogle gode råd til, hvilke tekniske sikringsforanstaltninger de kan etablere, og hvilke instrukser de kan nedfælde i virksomhedens it-sikkerhedspolitik for at undgå spam.

Vejledningen er disponeret som følger:

Beskrivelse af spam

Problemets omfang

Gener ved spam

Metoder til at høste mailadresser

Beskrivelse af adfærdsregulerende løsninger

Beskrivelse af tekniske løsninger

Markedsføringslovens bestemmelser vedrørende spam

Sammenfatning

Beskrivelse af spam

Spam defineres ofte på engelsk som unsolicited e-mail – hvilket direkte oversat betyder uanmodet e-mail. Denne definition er imidlertid ikke tilstrækkelig præcis, idet de fleste jævnligt får e-mails med informationer, som de ikke har anmodet om, men som alligevel er nyttige og anvendelige informationer – f.eks. en invitation til en fest eller en e-mail fra et ukendt familiemedlem.

I stedet vil vi definere spam som en rundskrivelse, der er modtageren uvedkommende i betydningen:

- modtageren har ikke bedt om at få den
- indholdet er ikke relevant for modtageren
- modtageren er ikke direkte relateret til indholdet eller afsender
- rundskrivelsen er kommunikeret til modtageren elektronisk

I pressen såvel som i denne vejledning er spam forbundet med e-mails. Spam kan ifølge vores definition imidlertid også komme i andre former som f.eks. sms og mms. Spam er dermed heller ikke kun tilknyttet PC'er, men kan forekomme på alle elektroniske enheder, der anvendes til kommunikation – f.eks. mobiltelefoner og håndholdte computere. Spam skal dog kun forstås som elektronisk kommunikation, og dermed er masseudsendelse af trykte reklamer altså ikke spam.

Mange typer spam er bygget op på samme måde. Der findes typisk en verifikation af afsenderen, som f.eks. kan være en kendt virksomhed eller en person med autoritet. Herefter kommer der en krog i modtageren, som f.eks. får et godt tilbud, som vedkommende burde benytte sig af. Dernæst ser man tit en form for trussel i den betydning, at noget vil gå galt for modtageren eller andre, hvis man ikke benytter sig af tilbuddet. Endelig er der ofte en opfordring til at distribuere mailen videre.

Eksempler på spam inkluderer:

- Nigeriabreve, som er opfordringer til at hjælpe en nødstedt person med et eller andet mod en klækkelig betaling
- Reklamer, som opfordrer modtageren til at købe et bestemt produkt eller en bestemt service
- Kædebreve, der altid indeholder et eller andet budskab, som man skal sende videre
- Hoaxes, som typisk er advarsler om et eller andet – f.eks. en virus – og som man opfordres til at sende videre
- Virus eller forskellige former for hackerværktøjer, som forsøges smuglet ind på computeren under dække af at være en af ovenstående typer spam

Der er ikke enighed om hvor ordet "spam" stammer fra. Oversætter man ordet direkte fra engelsk betyder det dåsekød, og refererer dermed til kød af dårligt kvalitet og af ukendt oprindelse. En anden version går på, at ordet stammer fra Monty Python sangen: "Spam spam spam spam, spam spam spam spam, lovely spam, wonderful spam...". Spam bliver i denne betydning en uendelig gentagelse af ligegyldig tekst. Endelig er der nogle der mener, at ordet stammer fra computerlaboratorierne ved University of Southern California, fordi spam har samme karakteristika, som de ansattes frokostkød:

- Ingen vil have det eller beder om at få det
- Der er aldrig nogle der spiser det – i stedet bliver det bare skubbet til side på tallerkenen
- En enkelt gang imellem har det en god smag – ligesom spam-mails der faktisk engang imellem kan være relevante.

Spam er blevet et problem fordi det er så let at sprede sit budskab til mange mennesker på en gang, fordi det kan gøres meget hurtigt, fordi omkostningerne er negligerbare for afsenderen, fordi det er let at måle effekten af mailens omfang og fordi det er meget fleksibel måde at komme af med sine budskaber på.

Problemets omfang

Den 3. juni 2003 citerede tidsskriftet Ingeniøren en ny undersøgelse fra sikkerhedsfirmaet MessageLabs, som viste, at ud af 133,9 millioner e-mails var de 51% spammails. Artiklen kan findes her: <http://www.ing.dk/apps/pbcs.dll/article?Dato=20030603&Kategori=IT&Lopenr=106060018&Ref=AR>.

Der er imidlertid store usikkerhedsmomenter ved at opgøre omfanget af spam. For det første fordi mængden af spam varierer noget ud fra, hvilken region i verden vi ser på. For det andet fordi de målinger, der er foretaget, stammer fra virksomheder, der allerede har tilmeldt sig en eller anden form for måling af problemet. Da disse virksomheder får fortalt sådanne målinger, må man forvente, at de allerede har fokus på problemet, fordi de i gennemsnit modtager større mængder af spam end virksomheder, der endnu ikke er så generet af problemet, at de har gjort noget ved det. For det tredje fordi der er en vis usikkerhed ved at opgøre, hvad der faktisk falder under betegnelsen spam. Vi vil derfor se på en flerhed af forskellige kilder med henblik på at estimere omfanget af spam.

EU-kommissionen har vurderet at det globale omfang af spam overstiger 50% af alle mails. Samtidig vurderes det, at produktivitetstab i europæiske virksomheder i 2002 som følge af disse mængder spam var på 2,5 milliarder euro. (se bl.a. <http://www.comon.dk/index?page=news:print,id=14576> og <http://www.computerworld.dk/default.asp?Mode=10&ArticleID=19865>).

Gartner forudsagde i 2002 (J. Graff og M. Grey, Management Alert: 2003 E-Mail Predictions Highlight the Rising Risk Factor, Gartner, 4. december 2002), at spam ville stige eksponentielt med en stigningsrate på 1000% p.a., og at mere end 50% af al elektronisk kommunikation vil være spam i 2004 (0,8 sandsynlighed). På området e-mail er dette altså allerede nået i år, hvis vi skal tro opgørelsen fra MessageLabs. Tilsvarende forudsagde Gartner, at produktiviteten vil falde som følge af denne store mængde kommunikation, at vi vil se et stigende antal retssager som følge af kommunikation og at

markedet for anti-spam produkter vil konsolidere sig i løbet af 2003. Flere internationale analysebureauer peger på, at mængden af e-mails vil eksplodere gennem de kommende år. Således går bud fra internationale analysebureauer på at en funktionær i dag modtager i gennemsnit 55 e-mails om dagen. Det betyder, at uafhængigt af spam, vil der i fremtiden være behov for automatiserede systemer (e-mail response management system, ERMS) til at analysere og evt. besvare disse store mængder af mails.

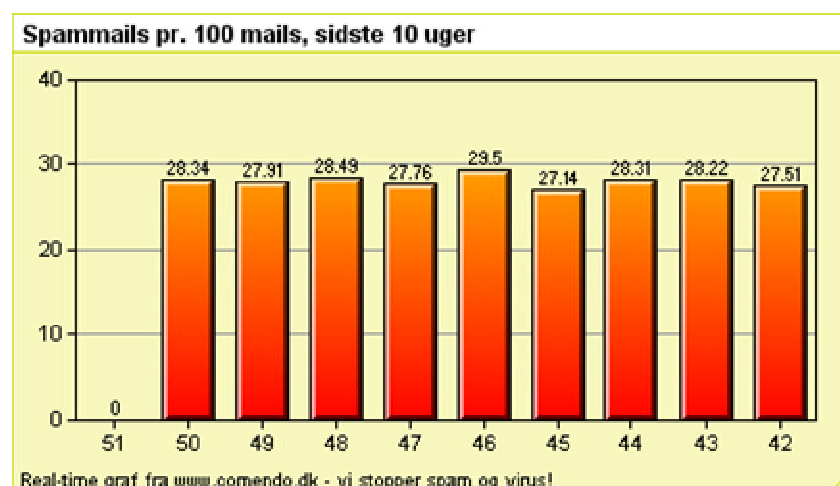
Endelig kan man fremhæve Center for Democracy & Technology's undersøgelse, <http://www.cdt.org/speech/spam/030319spamreport.pdf>, hvor 8.842 ud af lidt over 10.000 modtagne e-mails var spam. I denne undersøgelse havde man dog også gjort mange ting for at tiltrække spam, og derfor må tallet på 88% af alle mails anses for at være højt.

Der findes ikke danske tal for antallet af e-mails, der afsendes i Danmark om dagen. Tilsvarende findes der heller ikke en opgørelse over antallet af funktionærer. Vi kan estimere antallet af personer i Danmark, der må forventes at afvikle væsentlige dele af deres job foran en PC til at være 1.300.000 - se udregning her. Hvis vi på linie med ovenstående antager, at en funktionær modtager 55 e-mails om dagen, til danske forhold og antager, at der er 1.300.000 relevante personer og 220 arbejdsdage, kan vi få et skøn over det absolutte antal e-mails, der sendes i Danmark om året i arbejdsrelateret henseende: 55 e-mails * 220 arbejdsdage * 1.300.000 personer = 15.730.000.000 e-mails om året. Heraf skulle omtrent halvdelen være spam. Det er dermed indlysende, at vi står overfor et væsentligt problem, der både i forhold til medarbejdernes arbejdstid med at læse spammails og i forhold til nettets kapacitet er rent spild.

Billedet bliver endnu værre, hvis man i stedet for blot at se på e-mails også medregner andre elektroniske kommunikationsformer. Ifølge en undersøgelse offentliggjort i IT- og Telestyrelsens Teleårbog (<http://www.itst.dk/static/teleaarbog/2002/html/chapter02.htm>) blev der i 2002 sendt 2.018.654.000 sms'er. Denne kommunikationskanal er endnu ikke så voldsomt udsat for spam som e-mails. Men i en ikke alt for fjern fremtid vil spam sandsynligvis også gøre et voldsomt indtog på denne kanal, med risiko for at gøre den uanvendelig.

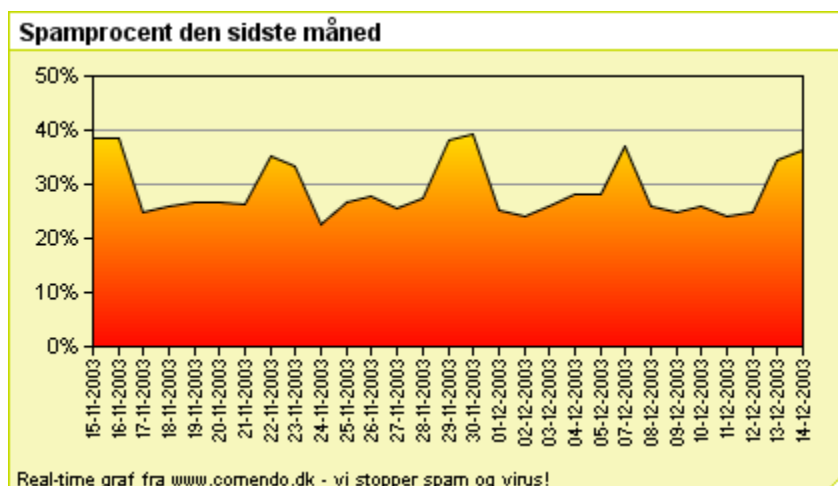
Ser vi udelukkende på danske tal, er det ganske tydeligt, at problemet i Danmark indtil nu har været mindre, end det gør sig gældende i såvel USA som verden i gennemsnit.

Den danske virksomhed comendo foretager dagligt spamfiltrering af ca. 300.000 mails for ca. 1100 kunder (tal fra 2003). Ifølge disse oplysninger er knapt en tredjedel af alle mails spam. Det fremgår bl.a., når man ser på et tilfældigt udvalg af uger i 2003.



Figur 1: Spammails i procent af samlet antal mails i perioden uge 25-34, 2003.

Et tilsvarende billede får man, hvis man kigger på antallet af spammails i procent af det samlede antal mails i en given måned.



Figur 2: Spammails i procent af samlet antal mails i perioden 23. juli 2003 til 21. august 2003.

Figur 2 viser en del fluktuationer i antallet af spammails. Disse fluktuationer dækker over, at mængden af mails reduceres i weekender, mens mængden af spam-mails ikke reduceres, og derfor kommer til at dække over en større procentdel. De pågældende statistikker kan i de nyeste versioner findes på: <http://www.comendo.dk>.

I anledning af den internationale antispamdag den 22. maj 2003 er der også lavet en oversigt over, hvilke lande der er den største kilde til spam på de danske systemer. En top-ti som ser ud som følger:

Rangordning	Land	Procent
1	USA	38,59
2	Kina	12,24
3	Korea	8,64
4	Brasilien	4,32
5	Canada	3,28
6	Storbritannien	2,24
7	Danmark	2,18
8	Sverige	2,16
9	Tyskland	2,04
10	Spanien	1,83
Øvrige	Alle andre lande	22,48

Dette resultat afspejler at kilderne til spam fortrinsvis er fra lande, der ikke har regulering af, hvordan man må foretage elektronisk markedsføring, at de servere der bruges til at afsende spammails fra fortrinsvis er placeret i de udviklede lande (hvor man kan oprette en gratis mailkonto), og at der er en overvægt af spam fra lande som Danmark i størst omfang må forventes at have kontakt med. Jo mere en virksomhed har elektronisk kontakt til udlandet, jo mere spam må den forventes at modtage.

Man kan også se på, hvilke typer af spammails der bliver stoppet af comendo. En undersøgelse viser, at der er tale om mange forskellige typer af mails. Ved den internationale spamdag havde comendo således stoppet 73.445 forskellige mails. Eksempler inkluderer følgende emner:

Adobe Photoshop, over 85% off retail.. save over \$400!

Earn a six-figure income from home with Ebay!

Unlimited adult DVD downloads, for free..

Mortgage Approved... get the home loan you deserve – lowest

40% off the leading AntiVirus software in the world...

Someone Sent You An Instakiss! See who!

You can order Anti-depressants, weight loss meds, and pain...

Viagra, Phentermine, Xenical & many others prescribed online

Cum watch med play =)

Det er dermed en skøn blanding af produkter, services, medicin og porno som tilbydes blandt de mest hyppigt forekommende spammails.

Gener ved spam

Mange virksomheder har den holdning, at spam er hurtigt at identificere i indbakken og endnu ikke et så stort problem, at man gider gøre noget ved det. Men en sådan intuitiv vurdering af spam skal man ikke nødvendigvis forlade sig på. I stedet er det vigtigt at se på de elementer af spam, som kan være med til at genere virksomheden.

Spam kan være mentalt generende for mange mennesker. En del mennesker bliver provokeret af at få tilsendt pornografisk materiale, tilbud på hormoner, potensforbedrende eller penisforstørrende midler eller nervemedicin. Sådanne meddelelser krænker den privatsfære, som folk føler, at de har i forhold til sådanne emner. Andre mennesker vil derimod føle sig unødigt draget af dem og tilbringe en del af arbejdstiden med at gennemgå dem.

Man kan måske også argumentere for, at der er et socialt ansvar for at beskytte unge mennesker og svage individer mod de tilbud, som fremkommer via spammails. Tilsvarende kan man også argumentere for, at det ikke er fornuftigt for de fleste mennesker at bruge deres fritid på at skulle sortere spammails fra.

Netværksbelastningen udgør også et problem. For at håndtere den stadig stigende mængde spam kræves der øget båndbredde på internettet og større og stærkere mailservere og netværk i virksomheden. Den store mængde spammails kan simpelthen reducere netværkenes stabilitet betydeligt.

Ondsindet kode i forbindelse med spam kan føre til store omkostninger for virksomhederne. Man ser i stigende grad at spam er et dække for forsøg på at smugle ondsindet kode ind i virksomheden – enten direkte i forbindelse med mailen eller i forbindelse med links til hjemmesiden, hvor koden hentes. Den ondsindede kode kan være orme, virus, trojanske heste, programmer, der har til formål at afsløre virksomhedens netværksinfrastruktur eller at bevise at mailadressen stadig er i live, eller lignende.

Endelig er der den tid, som medarbejderne bruger på at frasortere spam i deres indbakke. De fleste tror, at de kan gøre det på et par sekunder, men processen tager som regel længere tid. Et almindeligt scenarie er, at man sidder og arbejder på sin computer. Så ankommer der en e-mail, et signal lyder, og man afbryder arbejdet for at skifte til mailprogrammet for at læse den nye mail. Afhængigt af, hvor god spammailen er, tager det fra et par sekunder til et halvt minut at identificere, om der er tale om en spammail. Hvis det er en spammail, og man beslutter sig for at stoppe med at læse indholdet, så snart man har identificeret den som værende en spammail, skal man lukke mailen og slette den. Herefter skal man over i det program, hvor man tidligere arbejdede og finde ud af, hvor man var nået til, og hvordan man kommer videre med arbejdet. Undersøgelser viser, at det for den almindelige medarbejder tager 30-40 sekunder at modtage en spammail. Hvis vi antager, at hver medarbejder modtager 55 mails om dagen, hvoraf halvdelen er spam, koster det hver medarbejder $27 \text{ mails} * 30 \text{ sekunder} =$

13,5 minutter om dagen at frasortere spammails – og det er forudsat, at medarbejderne ikke læser indholdet. Antager vi, at medarbejderne får 150 kroner i timen, koster det virksomheden 33,75 kroner pr. medarbejder pr. arbejdsdag at modtage spammails. Hertil skal så lægges de omkostninger, som den ekstra netværkskapacitet og eventuelle manglende netværksstabilitet koster. Og endelig skal der lægges det ubehag medarbejderne føler ved at modtage spammails. Spam koster virksomhederne dyrt på bundlinien.

I nogle lande holdes arbejdsgiveren ansvarlig for de gener en medarbejder påføres ved at modtage spam på arbejdspladsen. Det gælder særlig, hvis arbejdsgiveren ikke har gjort, hvad der må anses som værende rimeligt muligt for at frafiltrere spam. Et sådant forsøg på at holde arbejdsgiveren moralsk ansvarlig for spam gør sig endnu ikke gældende i Europa. I Danmark har arbejdsgiveren således ikke et objektivt ansvar for at sikre at medarbejderne ikke modtager spam. Men det er muligt, at det kommer i fremtiden, og det kan derfor være relevant at have forberedt sig.

Metoder til at høste mailadresser

Personer der gerne vil sende spam anvender flere forskellige metoder til at få fat i de mailadresser, de gerne vil sende til.

- De scanner hjemmesider og nyhedsgrupper for mailadresser ved at anvende høstmaskiner som f.eks. Atomic Harvester, Perfect E-mail Harvester og Power E-mail Harvester. Denne metode er ifølge en undersøgelse fra Center for Democracy & Technology, <http://www.cdt.org/speech/spam/030319spamreport.pdf>, den største kilde til at modtage spam.
 - De køber lister med mailadresser.
 - De prøver sig frem med bogstavkombinationer – f.eks. aaa@ditfirma.com, aab@ditfirma.com, aac@ditfirma.com osv.
- Alternativt kan de også prøve med små korte eller sandsynlige navne som jens@ditfirma.com.

Beskrivelse af adfærdsregulerende løsninger

Selv om spam koster virksomhederne dyrt på bundlinien behøver det ikke koste en formue at bekæmpe spam. Man kan nå langt i at reducere mængden af spam i indbakken ved at anvende en række forholdsvis simple adfærdsregulerende regler.

Adfærdsregulerende foranstaltninger

a. Der er sammenhæng mellem ledelsesansvar og it-sikkerhedspolitik

Ligesom med alle andre it-sikkerhedsinitiativer, er det ledelsens ansvar at udstikke de retningslinier, der skal til for at sikre virksomhedens elektroniske data og elektroniske kommunikation. Herunder er det også ledelsens ansvar at fastsætte en politik for såvel indgående spam som udgående elektronisk markedsføring. Reglerne for den udgående elektroniske markedsføring, der forhindrer at virksomheden selv bliver en spammer, kan der læses mere om i afsnittet om markedsføringsloven. Reglerne for den indgående spam skal nedskrives i virksomhedens it-sikkerhedspolitik. Reglerne skal dels omfatte en stillingtagen til, hvilke tekniske sikkerhedsforanstaltninger der skal erhverves, og dels en stillingtagen til, hvilken adfærd medarbejderne bør iagttage for at virksomheden ikke skal udsættes for spam. Det præcise indhold af denne politik er genstanden for dette og det følgende afsnit.

b. Vurder i hvilket omfang virksomheden skal beskyttes

Virksomheden bør tage stilling til, i hvilket omfang den vil beskytte sig. Virksomheden bør dermed tage stilling til:

- hvordan den vil definere spam
- hvor stort et omfang virksomheden kan tolerere i forhold til netværkets og servernes kapacitet
- om der er bestemte typer af spam, den slet ikke kan tolerere

- hvilke omkostninger virksomheden er villig til at bære (tag f.eks. udgangspunkt i ovenstående beregninger)
- hvilke segmenter af virksomheden skal beskyttes i forhold til andre
- om virksomhederne vil opstille specielle computere på virksomheden, som medarbejderne kan anvende til private formål.

c. Bør ansatte oprette en gratis webmailkonto

Virksomheden skal tage stilling til, om det kan tillades at virksomhedens medarbejdere bruger den mailkonto, de har fået på virksomheden til private formål. Herunder skal der også tages stilling til, om medarbejderne skal opfordres til at oprette en gratis webbaseret mailkonto til private formål – eller måske endog til visse dele af det arbejde, der sker for virksomheden. F.eks. kan man anbefale medarbejderne at oprette en speciel webmailkonto til nyhedsbreve og anvendelse i nyhedsgrupper, som ofte i særlig grad er ofre for spam. Fordelen ved dette er, at virksomhedens egne it-installationer ikke belastes af trafikken, og at sandsynligheden for at der kommer spammails til medarbejdernes formelle virksomhedsmailskonto reduceres. Men spammails kan naturligvis også ramme den webbaserede e-mail. Samtidig skal virksomheden være opmærksom på, at mails der læses i en browser, typisk ikke er underlagt samme sikringsforanstaltninger som mails der læses i en egentlig mailklient. F.eks. har mange virksomheder valgt at mails med vedhæftede filer med bestemte ekstensions (.vbs, .exe, m.v.) ikke kan modtages og får den vedhæftede fil fjernet eller lignende. Men disse regler gælder sjældent filer, som downloades fra internettet og dermed filer der hentes ned gennem en webbaseret mailklient. Hvis virksomheden anbefaler webmails, skal der tages højde for sådanne forhold. Det anbefales at virksomheden hjælper de ansatte til at få en privat webmail, som er beskyttet i overensstemmelse med it-sikkerhedspolitikken. Det kan f.eks. ske ved at virksomheden opstiller en mindre mails server til dette formål.

d. Retningslinier for hvad folk må tilmelde sig med deres virksomhed mailkonto

Der skal laves retningslinier for, om medarbejderne må tilmelde deres formelle virksomhedskonto til nyhedsbreve og nyhedsgrupper. Begge dele er ofte kilder til store mængder spam, men kan være særdeles nyttige i arbejds mæssigt henseende.

e. Undlade at besvare spam

Det skal anbefales medarbejderne aldrig at besvare spammails – heller ikke selv om der er link til afmelding af den pågældende spam. Ofte er et sådant link nemlig blot et forsøg på at finde ud af, om den pågældende mailadresse stadig fungerer og bliver læst. Hvis spammeren får vished for dette, kan det kun føre til mere spam.

f. Beskyttelse af kundekartoteker

Virksomheden skal være klar over, at dens kundekartoteker er omfattet af persondatalovens bestemmelser om handel med adresser og videregivelse af data. Det er ulovligt uden samtykke, og derfor bør virksomheden aldrig sælge eller videregive sådanne kartoteker.

g. Læs privacy politik

Hvis det er nødvendigt at bruge sin mailadresse til at tilmelde sig noget på en hjemmeside er det vigtigt at læse den privacy politik, som bør være specificeret på den pågældende hjemmeside. Man bør især være opmærksom på, om det er muligt at framelde sig en eventuel service og om virksomheden deler ud af mailadresse informationer til partnere. Faktisk viser statistikkerne at stort set alle virksomheder, der har en privacy politik, overholder den, <http://www.cdt.org/speech/spam/030319spamreport.pdf>.

h. Videre send ikke spam

Mængden af spam er i forvejen meget stor. Det nytter derfor ikke at gøre denne mængde endnu større ved at videre sende spam til andre - uanset hvor tillukkende de tilbud man måtte modtage lyder. Folk, der modtager spam, kan se, hvor det kommer fra, og det kan give et u hensigtsmæssigt image af den enkelte afsender samt dennes virksomhed.

i. Opret en intern e-mail adresse til spam

Virksomheden bør oprette en intern e-mailadresse, som medarbejderne kan videresende spammails til. Formålet er at systemadministratoren kan anvende de indkomne spammails til at blokke for lignende spammails.

Beskrivelse af tekniske løsninger

Der eksisterer allerede i dag en række tekniske løsninger, som stort set fejlfrit kan sortere i mængden af mails. Virksomheden bør vurdere, om sådanne løsninger skal erhverves.

a. Skal virksomheden håndtere spam selv eller købe løsning hos leverandør

Når virksomheden har besluttet sig for, at der skal gøres noget teknisk ved den mængde af spam den modtager, er der to muligheder: enten selv at skaffe sig en boks eller et program til at håndtere problemet eller at få opgaven løst af leverandører udefra.

Virksomheder kan købe forskellige tekniske løsninger, som placeres på netværket, og som fungerer til at sortere spam fra. Der er mange forskellige typer afhængigt af ens behov, og hvilken leverandør man kontakter. Boksene kan indeholde mange forskellige funktioner. F.eks. kan man få antivirus scanner, spamfilter, indholdsfiltrering, sikker web-mail m.v. i én boks. Boksene er også forskellige i forhold til, i hvor høj grad de kan passe sig selv. Nogle af dem skal opdateres en gang om ugen med nye filtre – andre opdaterer sig selv over internettet.

Fælles for boksene i forhold til spam er, at de er baseret på et eller flere filtre. Der er mange forskellige typer af filtre afhængigt af, hvad man ønsker:

- Et filter indeholder alle kendte afsenderadresser af spam. Filtret opdateres hele tiden via internet således, at hver gang det bliver kendt, at en spammail er udgået fra en bestemt mailadresse, så vil denne mailadresse blive blacklistet, og man vil ikke længere kunne modtage mails fra adressen.
- Et andet filter er baseret på genkendelse af allerede kendte spammails. På baggrund af den kendte spammail, som så snart den er kendt, blacklistes, genereres en checksum, som så efterfølgende sammenlignes med alle de mails, der går ind på virksomhedens mailserver. Er en indgående mail identisk med en kendt spammail fjernes den så fra serveren.
- Et tredje filter er baseret på det princip, at antallet af gange en given mail er blevet set på internet, er en god indikation af, om det er en spammail. Hvis en given mail er set f.eks. en million gange, kan man sørge for at få den sorteret fra.
- Et fjerde filter måler på, om en mail er fra en nyhedstjeneste, hvilke farver bogstaverne i mailen har, om der anvendes bestemte spamvendinger, osv. På denne baggrund bestemmes det, om der er tale om en spammail.
- Et femte filter analyserer kendte spammails og bestemmer på baggrund heraf nogle fællestræk for spammails. Disse fællestræk bruges til at identificere og eventuelt klassificere lignende mails som værende spam. Filtret analyserer alle indgående mails og lærer derved hvilket sprog, der bruges hos virksomheden. Dette bidrager til, at meget afvigende mails kan sorteres fra. F.eks. er det ret sandsynligt at ordet Creditcard er spam, hvis det bliver sendt til en glarmester, men meget usandsynligt, hvis det bliver sendt til en bank.
- Den sidste type filtre er dem, man selv kan konfigurere på baggrund af egne intuitive erfaringer. Her kan man f.eks. sørge for at blacklist eller whiteliste visse afsendere. Det betyder, at hvis man f.eks. ikke ønsker at modtage mails fra bestemte afsendere, kan man blacklist dem, og hvis der er nogen, som man altid gerne vil have mails fra, kan man whiteliste dem. Grundlæggende handler det om at gøre sig overvejelser om, hvem der er virksomhedens venner og fjender, og hvordan, hvorfor og hvornår.

Som nævnt er det kun én mulighed at indkøbe en sådan boks og placere den på netværket: man kan også vælge at få sine mails sorteret inden de kommer ind i virksomheden. En række virksomheder påtager sig at sortere ens mails for virus, orme, spam m.v. De bruger samme teknikker som ovenstående bokse, men fordelene er naturligvis, at man ikke selv skal have boksen stående, men i stedet kan

regne med, at andre har foretaget de nyeste opdateringer og kan skride ind med manuelle tiltag, hvis f.eks. et af de store ormeudbrud skulle gå i gang. Desuden fanges mailen inden den når ind og bruger båndbredde og lagerkapacitet på mailservoren. Ulempen ved denne løsning er, at man principielt set krænker den privacy, som de pågældende mails forventes underlagt, idet den valgte leverandør vil kunne gøre sig bekendt med indholdet af de mails han scanner. Desuden vil visse systemadministratorer foretrække selv at kunne eje og håndtere hardwaren, planlægge og styre sine infrastrukturbehov og endelig kan organisationen generelt være modstander af outsourcing.

Hvis man vælger en løsning med filtrering af spam skal man være meget forsigtig med, hvordan man konfigurerer sine filtre. Er man for restriktiv, eller ender ens kunder på listen over spamafsendere, vil man ikke kunne modtage de mails, man har behov for at drive sin forretning. Filtrene skal derfor udformes med stor bevågenhed og de skal vedligeholdes.

Hvis man vælger en ekstern leverandør routes virksomhedens mails først over den eksterne leverandør inden de kommer ind i virksomheden. Hvis man løser opgaven selv kan man vælge tre fremgangsmåder:

1. At installere et antispam produkt på virksomhedens SMTP relay server (som ikke nødvendigvis er e-mail server).
2. At installere et antispam produkt på virksomhedens e-mail server (som så antages også at være SMTP relay server). Tillige hermed at anvende de antispam services, der måtte være indbygget i mailservorens software.
3. At styre antispamsoftware på desktopniveau gennem det software, der evt. måtte høre til e-mail klienterne.

b. Redegøre for hvad man kan forvente sig af filtre i allerede anskaffet software og hardware

Flere af de produkter, som virksomheden allerede i dag er i besiddelse af, indeholder muligheder for at filtrere, ihvertfald visse dele af spam fra.

b1. Lotus

Lotus Domino indeholder en række elementer til at håndtere spam. Der er mulighed for dels at håndtere dette på server niveau, således at det ikke er den enkelte bruger, der skal tage stilling til, hvorvidt den modtagne post er spam, men derimod en egentlig virksomhedsbeslutning. Derudover har den enkelte bruger ligeledes mulighed for at luge det spam ud, der eventuelt slipper igennem de kriterier, som er stillet op af virksomheden.

På server siden stiller Lotus Domino følgende faciliteter til rådighed:

- Server post regler
- DNS blacklist filtre
- Restriktioner på muligheden for at fungere som relay, altså at fungere som post-gennemstillingscentral
- Blokering og kontrol af Internet-baseret post

I det følgende gennemgås de enkelte elementer omtalt i ovenstående oversigt:

Lotus Domino serveren

Serverbaserede postregler

Til håndtering af spam, kan man på server-niveau - altså der hvor posten ankommer - sætte en række kriterier, der definerer håndtering af posten. Udgangspunktet er her, at der kan defineres de karakteristika, der definerer spam.

Dette omfatter således check på:

Hvem er afsenderen

Hvad er postens overskrift

Hvad står der i selve indholdet

Hvilket internet domæne kommer posten fra

Hvor stor er denne

Hvilke vedhæftede filer er der (navn og antal)

Disse kriterier kan benyttes enkeltvis eller i ønskede kombinationer, og på basis af disse kan man definere hvorvidt posten kan nægtes modtagelse eller flyttes i karantæne.

Igen skal det fremhæves, at dette ikke kræver brugerinvolvering, men håndteres af administratoren.

DNS blacklist filtre

DNS-blacklists er eksterne databaser, der løbende holder øje med hvilke SMTP-værter, der bør betragtes som kilder til spam. Med udgangspunkt i disse kan Lotus Domino checke hver enkelt modtagne post, og dermed definere, hvad der skal ske med denne post; altså om denne skal afvises eller på anden måde forhindres aflevering til den egentlige modtager. I og med at denne offentlige service løbende opdateres, vil dette lette arbejdet for den enkelte virksomhed.

Restriktioner for at fungere som relay

En af de mere elegante måder at udsende spam på er at lade et andet 'postkontor' fungere som viderestilling, og dermed skjule postens oprindelse. Dette er uønsket af to årsager, idet det forhindrer restriktionerne på afsender-niveau og dels fordi det lægger en uønsket belastning på virksomhedens postinfrastruktur. Ydermere - og måske allerværst - vil det få virksomheden til at fremstå som spammer!

I Lotus Domino er der derfor flere muligheder for at undgå denne situation, idet man blandt andet kan indlægge kontrol på hvilke internetdomæner, som kan sendes til, og hvilke internethosts, der accepteres. Hermed kan man undgå at fungere som postkontor og potentiel spammer.

Blokering og kontrol

Udover de ovennævnte muligheder er der andre mekanismer, der kan benyttes i tillæg. For det første kan man definere, hvorvidt den enkelte bruger overhovedet skal kunne modtage Internet baseret post. I dagens Danmark er dette nok ikke en realistisk mulighed, udover for enkelte brugere. For det andet kan man checke, hvorvidt den ønskede modtager overhovedet eksisterer, og derefter automatisk slette post, der må siges at være udsendt med spredhagl. Endelig kan man definere, hvilke brugere, der kan modtage post fra hvilke Internetdomæner.

Lotus Notes klienten

Brugersiden

Selvom der med disse serverbaserede muligheder kan undgås en stor del af den daglige spam, vil der under alle omstændigheder slippe noget igennem til den enkelte bruger. Det er jo altid et valg, hvor restriktiv man ønsker at være opvejet mod, at der rent faktisk er post, man ønsker at modtage. Så på serversiden vil dette altid være en balancegang, og dermed skal brugeren have mulighed for selv at kunne forfine egne restriktioner.

Dette er også muligt i Lotus Domino, eller nærmere betegnet i Lotus Notes klienten.

Brugeren har således mulighed for at lave sine egne regler til håndtering af post, og dermed også definere posthåndtering svarende til de serverbaserede postregler. Brugeren kan altså selv vælge at slette post baseret på afsender, postindhold indhold, Internetdomæne med videre.

Afhængig af den skadevirkning, man tilskriver spam, er der med de ovennævnte muligheder mange muligheder chancer for at minimere spam i virksomheden. Spam bliver på denne måde udsat for to sæt filtre, nemlig dels de serverbaserede som er administratorens ansvar og generelt gældende for hele virksomheden og derefter den enkelte brugers yderligere forfining via eget regelsæt.

b2. Microsoft

Microsoft er gået meget aktivt ind i bekæmpelsen af spam. Både ved at forbedre og videreudvikle anti-spam foranstaltningerne i egne produkter samt ved at gå sammen med nogle af industriens andre ak-

tører - Yahoo! og AOL. Formålet med samarbejdet er bl.a. at udarbejde et best practice kodeks, hvor industrien sætter retningslinierne for, hvordan man sender kommercielle e-mails. Endelig er Microsoft gået juridisk til værks og har for nylig anlagt 15 retssager mod spammere. Og flere er på vej.

Indbygget spam-filter i eksisterende produkter

Den fornuftigste måde at bekæmpe spam på er at sørge for, at beskederne slet ikke når frem til de tilfældige modtagere, som spammerne forsøger at kontakte. Brugere af Microsofts produkter har i dag adgang til en række våben for at undgå dette.

Uanset om du bruger Microsoft Outlook, Outlook Express eller du har en hotmailadresse på <http://msn.dk>, så har du adgang til et professionelt spam-filter. Det fungerer på den måde, at du aktiverer og indstiller det indbyggede spam-filter, hvorefter emailklienten sorterer alle de emails, du modtager.

Guide til hvordan du udnytter det indbyggede spam-filter i Microsofts produkter

Nye anti-spam foranstaltninger med Exchange Server 2003

Microsoft har udviklet en række nye anti-spam værktøjer, som lanceres i efteråret 2003 sammen med Exchange Server 2003. Disse værktøjer vil hjælpe virksomhederne til at begrænse den tabte arbejdsfortjeneste i forbindelse med spam.

En funktionalitet gør det bl.a. muligt at skanne alle indkomne emails og give dem en score (Spam Confidence Level), som angiver sandsynligheden for, at det drejer sig om spam. Baseret på nogle kriterier defineret af administrator, vil emailen herefter enten blive sendt til modtagerens indboks eller blive dirigeret direkte til en junk mail folder. På denne måde undgår man, at medarbejderne hver dag må bruge tid på at sortere uønsket mail fra i deres post.

Læs mere om de nye anti-spam foranstaltninger i Exchange Server 2003 på:
<http://www.microsoft.com/presspass/press/2003/Apr03/04-14AntiSpamPR.asp>.

Outlook 2003 Exchange Server 2003 arbejder direkte med anti-spam filtre i den nye version af Outlook, som ser dagens lys i efteråret 2003. Outlook 2003 indeholder en række funktionaliteter, som vil bidrage til bekæmpelsen af spam.

Et avanceret "junk email filter" sorterer automatisk uønskede emails fra, baseret på en række forskellige kriterier: indhold, struktur, afsendertype m.m. På en "safe senders list" kan man selv angive de afsendere, hvis emails man under alle omstændigheder ønsker at modtage. Man kan f.eks. vælge kun at modtage emails sendt fra afsendere på denne liste, så man får fuld kontrol over den post, som havner i din indbakke. På en "block senders list", kan man desuden angive de afsendere, som man under ingen omstændigheder ønsker at høre fra.

Dette er blot nogle af de anti-spam foranstaltninger, som er indeholdt i Outlook 2003. Du kan læse mere på <http://www.microsoft.com/office/preview/editions/junkmail.asp>.

For mere information:

[Læs mere om, hvordan Microsoft bekæmper spam \(engelsk tekst\)](#)

b3. Novell

Novell GroupWise - en groupware platform der tilbydes til Windows, NetWare og snart også Linux servere (primo 2004) - tilbyder en politikstyret spam-håndtering på flere niveauer, for bedre at kunne tilgodese individuelle virksomheders forskelligartede behov. De teknologier, der i den sammenhæng benyttes til at identificere og håndtere spam, kan enten leveres indbygget direkte i GroupWise (fra og med version 6.5) eller af forskellige 3. parts leverandører som et add-on produkt til GroupWise. Disse anti-spam løsninger til GroupWise muliggør, f.eks. etablering af en **anti-spam Gateway** i forbindelse med virksomhedens GroupWise-system eller outsourcing af denne funktion til en ekstern service provider, hvis man foretrækker det. En alternativ løsningsmulighed, som tilbydes, er at etablere en **anti-spam service**, der direkte integreres med virksomhedens GroupWise domain- og posthus servere.

Metoderne som anvendes til identificering af spam kan f.eks. være på baggrund af afsenderinformationer - vha. manuelle/Realtime Blacklists (RBL) - eller på baggrund af indhold, såsom filtrering

på nøgleord, størrelse på eller type af vedhæftede filer samt heuristik. GroupWise 6.5 selv har en indbygget Blacklist-funktion til at identificere og håndtere spam. Anti-spam håndtering kan herunder f.eks. defineres på Internet Gateway niveau, hvor både manuelle (adresse) blacklists og en eller flere 3. parts RBL'er kan defineres for at beskytte sig imod spam. Samtidigt kan enhver GroupWise-bruger opsætte sine egne "positive" og "negative" lister, der enten tillader e-mail fra bestemte afsendere at komme igennem, afleverer dem i en Junk Mail folder eller automatisk sletter dem på posthus-niveau, **før** de når frem til brugerens indboks.

Brugen af blacklists har dog den medfødte skavank, at de kan være ressourcekrævende at definere og der er også en vis risiko for at der opstår et større eller mindre antal "falske positive" (dvs. et e-mail, der automatisk kategoriseres som spam, men som i virkeligheden ikke er det). Man kan dog med fordel kombinere Blacklist-funktionen i GroupWise med andre mekanismer i 3. parts anti-spam services, såsom førnævnte filtrering på nøgleord, størrelse på eller type af vedhæftede filer samt heuristik. Specielt heuristik-funktionen er interessant, idet den automatisk udsætter hver enkelt indkommende e-mail for en række test, der kan afgøre, hvorvidt der er tale om spam eller ej. Intensiteten af disse test(s) kan desuden øges eller mindskes efter behov og heuristik-rutinerne kan løbende tilrettes således, at de mere nøjagtigt kan afsløre lige netop den type spam, man på et givent tidspunkt belastes af. Heuristik kan i øvrigt også være et mere effektivt middel til at identificere nye typer af spam.

Den førende 3. parts anti-spam software understøtter GroupWise fra og med version 5.5 eller nyere, men mulighederne for nye sikkerhedsmæssige funktioner er blevet væsentligt forbedret i GroupWise 6.5 på grund af en ny og mere åben arkitektur. De samme produkter indeholder typisk også en række andre sikkerhedsmæssige funktioner, der f.eks. muliggør virus-eliminering, båndbreddekontrol, udvidede arkiveringsfunktioner, auditing samt andre sikkerhedsmæssige funktioner til GroupWise-systemet.

Læs mere om Novell GroupWise her: <http://www.novell.com/products/groupwise/>

b4. Sendmail

Sendmail er et program der fås til næsten alle operativsystemer, men bruges i udpræget grad på UNIX-systemer. Sendmail (og andre fortrinsvis UNIX-baserede programmer: Postfix, Qmail, Exim m.fl.) benyttes i udstrakt grad som gateway / relæ mellem virksomhedernes interne email-servere og Internettet. Sendmail leveres og opdateres af de fleste større hardware leverandører, eller kan hentes fra <http://www.sendmail.org/>.

Anti-spam i Sendmail kan opnås ved anvendelse af en lang række værktøjer og konfigureringsmuligheder. Som udgangspunkt er de nyeste versioner af Sendmail som default konfigureret til ikke at ville agere som åbent relæ, og sættet af email-regler og konfigurationsmuligheder opdateres løbende i takt med at nye versioner frigives. Alene af den grund anbefales det at holde Sendmail opdateret til nyeste version.

Sendmail (og Postfix, Qmail, Exim m.fl.) kan konfigureres til at yde en meget effektiv beskyttelse mod spam. Brugt i sammenhæng med indre email-servere og klienter med gode værktøjer, kan der opnås en særdeles kost-effektiv løsning med stor fleksibilitet for brugerne.

Protokol- og sanitets-tjek af afsenderen.

Sendmail er som udgangspunkt restriktiv m.h.t. formalia (overholdelse af protokoller og korrekt konfigureret domæner), men kan tunes til at være mere eller mindre restriktiv, - en skala rangerende fra "paranoid" til "ligegyldig". Desto mere insisteren på, at formalia skal overholdes, desto flere legitime sites vil ikke være i stand til at sende email til din gateway, med mindre de eksplicit hvidlistes. Omvendt, en relativt afslappet holdning til formalia kræver meget af de efterfølgende benyttede filtre. Tommelfingerreglen er: Restriktiv m.h.t. protokol giver større vedligehold og let konfiguration; Beskedne restriktioner m.h.t. protokol giver let vedligehold, men kompliceret konfiguration og risiko for selv at blive brugt som springbræt for spammere.

Filtrering på basis af afsender, afsender-system m.v.

Uden anvendelse af andet end Sendmail, kan der opereres både med hvidlister, sortlister, mønsterbaserede regler, opslag i interne og eksterne databaser. Filtringen kan specificeres både på basis af specifik afsender / modtager, systemnavne, domæner, og i nogen grad protokoller (se

http://www.sendmail.org/m4/anti_spam.html). Til forskel fra tidligere versioner af Sendmail, er det nu let at generere nye konfigurationer og teste dem uden at systemet skal tages off-line. At slå over på en ny konfiguration kan gøres "i farten", og der kan køres flere instanser af Sendmail med hver sin specifikke funktion og sæt af filtre. Det er også muligt at benytte 3'die-parts plug-in's, ligesom man kan skrive sine egne filtre (se http://www.sendmail.org/m4/adding_mailfilters.html).

Sendmail kan let konfigureres til at nægte at acceptere e-mails fra åbne relæer via specialiserede dns-opslag (f.eks. [Ordb: http://www.ordb.org/faq/](http://www.ordb.org/faq/)), ligesom den let kan anvende offentlige databaser over kendte spammere (f.eks. [Spamcop: http://www.spamcop.net/fom-serve/cache/291.html](http://www.spamcop.net/fom-serve/cache/291.html))

Filtrering på indhold

Indholdsfiltrering af enhver art er ikke umiddelbart en mulig konfigurationsoption for Sendmail. I stedet benyttes muligheden for ekstern filtrering enten via plug-in's eller ved at have flere sendmail-instanser kørende, der videregiver e-mailen til tredieparts-filtre og tilbage til sendmail. Et meget anvendt eksempel derpå er Spamassassin (se <http://spamassassin.taint.org/> og <http://www.ijs.si/software/amavisd/README.sendmail-dual>), der har en meget høj grad af sikker filtrering og inkluderer muligheden for at foretage virus-scanning inden e-mails når ind i virksomhedens indre e-mail-system. Spamassassin opererer med analyse af e-mailens header, tekst analyse (heuristik, nøgleord og lærte mønstre), sortlister og eksterne databaser over spam. Systemet kan udpakke og skanne de fleste former for kodning og komprimering. Spamassassin kan også operere i en tilstand hvor e-mail "læres" således, at der med meget stor sikkerhed kan skelnes imellem virksomhedens "normale" e-mails og "anormale" e-mails. For virksomheder med stort email-flow kan CRM114 (se <http://crm114.sourceforge.net/>) være et glimrende værktøj i sammenhæng med Sendmail og Spamassassin, netop i forbindelse med behovet for "læring". Sendmail kan også benytte eksterne servere (Exchange, Lotus m.fl.) til at foretage yderligere filtrering, arkivering og sortering m.v.

c. Spam i forbindelse med mobil opkobling

Flere og flere medarbejdere arbejder i marken eller derhjemme og anvender derfor mobil opkobling til arbejdspladsen. Disse opkoblinger er som regel mindre hurtige end internt i virksomheden, og derfor går der meget tid med at downloade ligegyldige beskeder. Virksomheden skal sikre sig, at også de mobile apparater beskyttes mod spam.

d. Undlad at anvende mailadresser på hjemmesider

Virksomheden bør overveje, hvordan den kan undgå at eksponere sine mailadresser, så de kan findes af disse scannere. Det kan ske ved kun at have én firmaadresse på hjemmesiden. Det kan også undgås ved slet ikke at have @ stående på hjemmesiden. Dette kan gøres ved at maskere sin mailadresse på hjemmesiden ved f.eks. at skrive aaaATditfirmat.com. Det kan også lade sig gøre ved at erstatte @ med en ISO-defineret kode: @ (se: <http://www.w3.org/TR/REC-html32>). Faktisk kan man gøre dette med hele mailadressen - f.eks. kan test@test.dk erstattes af test@test.dk. En generator til at disse erstatninger kan findes på: <http://www.wbwip.com/wbw/emailencoder.html>. Dette vil ikke blive genkendt af spammernes høstmaskiner og anvender man metoden viser undersøgelsen fra Center for Democracy & Technology, <http://www.cdt.org/speech/spam/030319spamreport.pdf>, at man helt kan undgå at modtage spam. Det er dog en stakket frist inden høstmaskinerne vil begynde at kunne genkende disse maskerede mailadresser. Man kan derfor alternativt anvende en mailadresse på hjemmesiden, hvor subject/emne feltet har en whitelisted tekst. På den måde vil kun mails med ét bestemt emne/subject få lov til at gå igennem mailfilteret. En sidste mulighed er slet ikke at anvende mailadresser på hjemmesiden, men i stedet at bruge formularer. Det betyder at afsender skal udfylde en formular på hjemmesiden – herunder med sin egen mailadresse for at få lov til at sende en mail igennem til modtageren.

e. Få digital signatur

Det skal anbefales at anvende digital signatur. Når man har oprettet en digital signatur er det sikkert, at man kan identificere hvem man er. Det betyder at en modtager af en e-mail med sikkerhed kan identificere afsenderen. Over tid kan dette være med til at begrænse spam, fordi dette typisk ikke vil blive sendt under anvendelse af en digital signatur. Digital signatur kan derfor være med til at sortere i mængden af spam.

f. Skjul din e-mailadresse

Hvis man gerne vil kommunikere med nogen på nettet, som beder om ens mailadresse, men samtidigt er i tvivl, om de vil misbruge ens mailadresse til at sende spam, kan man skjule sig bag en anden mailadresse. Princippet er således, at man opretter sig en ny mailadresse hos en udbyder af en sådan snydeadresse. Man opgiver så denne snydeadresse til den part, man gerne vil kommunikere med. Samtidig sætter man snydeadressen op således, at den router mails til en selv fra partneren til ens egentlige mailadresse, og samtidig således, at den router ens egne svar fra ens egen mailadresse til partneren igennem den adresse man gemmer sig bag. Hvis man så bliver spammet kan man nedlægge snydeadressen.

g. Undlad at have open relay mailservere

Mailservere kan afsende en mail fra sig selv til en anden mailservere uden, at hverken afsender eller modtager er tilknyttet den pågældende mailservere. Dette kaldes relaying. I praksis betyder dette, at man kan afsende en mail i en anden persons navn. Kombineres dette med en liste over modtagere, kan man altså uden at være tilknyttet den pågældende mailservere spamme løs. Mailservere bør sættes op således, at de kun kan afsende mails fra navngivne brugere i mailserveregens eget netværk. Som virksomhed er det muligt at teste om ens egen mailservere tillader open relaying. Det kan ske på <http://www.ordb.org>. Denne hjemmeside registrerer de mailservere der anvender open relay – uanset om der er testet eller ej. Hvis man ender på denne liste vil virksomheden ikke kunne kommunikere med en række mailservere rundt omkring i verden.

h. Udform mailadresser hensigtsmæssigt

Da meget spam bliver fremsendt ved at spammeren forsøger sig med simple bogstavkombinationer eller hyppigt anvendte navne, som jens@ditfirma.com, kan det anbefales at mailadresser er lange. jens@ditfirma.com kunne f.eks. i stedet hedde: jens.efternavn@ditfirma.com. Desuden må man anbefale at lade være med at bruge e-mailadresser med initialer af typen je@ditfirma.com.

Markedsføringslovens bestemmelser vedrørende spam

Lov om markedsføring blev ændret i sommeren 2003, efter at sagen om spam var blevet behandlet på europæisk plan. Lovændringen medførte at et nyt stk. 2 blev indsat ved § 4 i lov nr. 450 af 10. juni 2003 om ændring af lov om konkurrence- og forbrugerforhold på telemarkedet med flere love (Implementering af direktivpakken »99-review«). Stk. 2-6 i den gamle lov bliver herefter stk. 3-7. Bestemmelsen gennemfører dele af Europa-Parlamentets og Rådets direktiv 2002/58/EF af 12. juli 2002 om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor (databeskyttelsesdirektivet) (EF-Tidende 2002 nr. L 201, s. 37). Lovændringen er gældende fra 25.marts 2003. Lovændringen kan bedst forstås ved at se direkte på lovteksten.

Markedsføringslovens §6a før lovændringen

En erhvervsdrivende må ikke rette henvendelse til nogen ved brug af elektronisk post, et automatisk opkaldssystem eller telefax med henblik på afsætning af varer, fast ejendom og andre formuegoder samt arbejds- og tjenesteydelser, medmindre den pågældende forudgående har anmodet om det.

Nyt stk. 2

Markedsføringslovens §6a efter lovændringen

Uændret

Uanset stk. 1 kan en erhvervsdrivende, der fra en kunde har modtaget dennes elektroniske adresse i forbindelse med salg af en vare eller en tjenesteydelse, markedsføre egne tilsvarende produkter eller tjenesteydelser til kunden ved elektronisk post. Dette forudsætter dog, at kunden har mulighed for let og gebyr frit at frabede sig dette både i

forbindelse med afgivelsen af adressen til den erhvervsdrivende og ved efterfølgende henvendelser.

En erhvervsdrivende må ikke rette henvendelse til en bestemt fysisk person ved brug af andre midler til fjernkommunikation med henblik på afsætning som nævnt i stk. 1, hvis den pågældende over for den erhvervsdrivende har frabedt sig dette, hvis det fremgår af en fortegnelse, som udarbejdes af Det Centrale Personregister (CPR) hvert kvartal, at den pågældende har frabedt sig henvendelser, der sker i sådant markedsføringsøjemed, eller hvis den erhvervsdrivende ved undersøgelse i CPR er blevet bekendt med, at den pågældende har frabedt sig sådanne henvendelser. Ved telefonisk henvendelse til forbrugere gælder endvidere reglerne om uanmodet henvendelse i lov om visse forbrugeraftaler.

Uændret

Stk. 3 gælder ikke, hvis den pågældende person forudgående har anmodet om henvendelsen fra den erhvervsdrivende.

Uændret – bortset fra stk. henvisning

Første gang en erhvervsdrivende retter henvendelse som nævnt i stk. 3 til en bestemt fysisk person, der ikke er anført i fortegnelsen fra CPR, skal den erhvervsdrivende tydeligt og på en forståelig måde oplyse om retten til at frabede sig henvendelser som nævnt i stk. 3 fra den erhvervsdrivende. Den pågældende skal samtidig gives adgang til på en nem måde at frabede sig sådanne henvendelser.

Uændret – bortset fra stk. henvisning

Der må ikke kræves betaling for at modtage eller notere meddelelser om, at en anmodning efter stk. 1 tilbagekaldes, eller at henvendelser som nævnt i stk. 3 frabedes.

Uændret – bortset fra stk. henvisning

Erhvervsministeren kan fastsætte nærmere regler om den erhvervsdrivendes informationspligt efter stk. 5 og om pligten til at give adgang til at frabede sig henvendelser som nævnt i stk. 3.

Uændret – bortset fra stk. henvisning

Det helt centrale i lovændringen er, at virksomhederne før lovændringen aldrig måtte sende reklame-mails til en kunde, med mindre denne kunde direkte havde givet tilsagn hertil. Efter lovændringen må virksomhederne sende reklamemails til en kunde uden forudgående tilsagn, hvis:

- kunden har købt en vare eller service hos virksomheden efter lovens ikrafttræden
- kunden i forbindelse med varekøbet har opgivet sin mailadresse
- kunden i forbindelse med købet er blevet oplyst om, at han vil modtage reklamer og af hvilke kanal, han vil modtage disse
- kunden har haft mulighed for at sige nej tak
- kunden vederlagsfrit ved hver fremtidig modtagelse kan sige nej tak til at modtage mere
- virksomheden kun reklamerer for egne "tilsvarende produkter eller tjenesteydelser"

Sagt på en anden måde må virksomheden nu sende reklamemails til kunder uden et aktivt tilsagn fra kunden, hvis ovenstående betingelser er opfyldt. Det gjorde sig ikke tidligere gældende. Kunden skal nu aktivt melde fra – mens kunden tidligere aktivt skulle melde til.

Fortolkningen af loven indebærer bl.a.:

- Selv om markedsføringsloven gælder alle typer markedsføringskanaler gælder lovændringen kun markedsføring via e-mail, SMS, MMS og lignende, men ikke telefax og almindelig post.
- I en given reklame kan virksomheden søge kunden om samtykke til at måtte sende reklamer for andre produkter.
- Virksomheden må ikke anvende elektroniske adresser, der er oplyst af andre eller som virksomheden på anden måde er kommet i besiddelse af.
- Kunden skal have afgivet sin adresse i forbindelse med et køb – andre afgivne adresser er ikke omfattet loven.
- Virksomheden må kun markedsføre egne produkter - og altså ikke andre virksomheders produkter.
- Kunder der er optaget på CPR-registrets Robinson-liste (personer som har meddelt, at de ikke ønsker at modtage reklamer) er ikke omfattet af loven, og virksomheden må derfor også gerne sende reklamer til disse mennesker.
- Det er ikke tilladt via e-mail at indhente tilsagn fra kunden om, at denne vil modtage tilbud.
- Det vanskeligste ved loven er for virksomhederne at vurdere, hvad der er "tilsvarende produkter eller tjenesteydelser". Forbrugerombudsmanden giver nedenstående eksempler på, hvad der er lovligt. For hvert eksempel er der tilføjet en kolonne, som problematiserer disse eksempler ud fra en forventning om, hvad den pågældende forbruger signalerer har i øvrigt har brug for ved sit køb:

Har man købt...	Er det tilladt at reklamere for	Problematik
bukser	andet tøj	Herre/dame/børnetøj
musik-cd	andet musik, men ikke film	Musikvideo med samme band
sko	fodtøj, men ikke tøj	Herre/dame/børnesko
legetøj	legetøj, men ikke andre børneprodukter	Er computerspil legetøj
bil	andre biler, men ikke tilbehør eller service til biler	Man har næppe brug for endnu en bil, men kunne have brug for tilbehør
barbermaskine	andre elektroniske produkter til personlig pleje	Elektrisk tandbørste
sodavand	andre drikkevarer	
pc-spil	andre pc-spil, men ikke andet software	Styresystemer som betingelse for spillene

Forbrugerombudsmanden har forfattet et sæt regler, der kan anvendes som guide i forhold til hvilke rettigheder man har som forbruger, og i forhold til i hvilke situationer virksomhederne må fremsende reklamemails. Disse retningslinier kan læses her: <http://www.net-tjek.dk/ehandel/regler.htm>. Forbru-

gerombudsmanden uddyber disse retningslinier her: <http://www.net-tjek.dk/jura/fjura/jb00/00010000.htm> og her: http://www.net-tjek.dk/jura/lovereagl/mfl/rt_h00uh.htm.

Efter lovændringen har der været mange kritiske røster fremme om ændringen. Det frygtes nemlig fra mange sider, at lovændringen vil føre til stigende mængder af spam. Synspunktet er, at forbrugerne er blevet ringere stillet, fordi de ved ethvert varekøb skal framelde sig denne service, hvis de ikke ønsker informationerne. Det vurderes som en urimelig byrde for forbrugerne. Forbrugerne skal også betale for den tid, man er online, hver gang en sådan e-mail skal downloades til mailprogrammet. Samtidig fremføres også en frygt for, at mindre seriøse virksomheder vil vælge at anvende lempelsen af loven, fordi den forholdsvis begrænsede bøde, de kommer til at betale, ikke står mål med de eventuelle fordele ved at spamme (siden er den første danske spamdom dog faldet og her vurderede dommeren at det skulle koste omkring kr. 100,- pr. spammail, <http://www.bitconomy.dk/magasin.asp?printarticle=3012>).

Blandt skeptikerne er e-handelsfonden, der står bag det danske e-handelsmærke, som har besluttet, at de virksomheder, der har e-mærket, ikke må anvende de nye regler – jf.: <http://www.computerworld.dk/default.asp?Mode=10&ArticleID=19933>. Blandt andre skeptikere er dem, som mener, at reglerne endnu er ukendte for virksomhederne, og derfor i en indledende fase vil lede til mere spam: <http://www.comon.dk/index.php?page=news:print,id=15098>.

Tilhængerne af lovændringen argumenterer for, at det var positivt at direktivforslaget kom, fordi EU fik fælles regler på området. I mange lande havde man aldrig haft en beskyttelse af forbrugerne på dette område. Disse forbrugere er derfor blevet langt bedre stillet. Desuden kan man argumentere for, at lovændringen er i tråd med nyere og meget effektive forretningsmodeller. Hvis man f.eks. har købt et produkt, som der kommer en opdatering eller noget ekstra udstyr til, vil de fleste forbrugere være glade for at kunne modtage disse informationer automatisk frem for ved hvert varekøb, at skulle huske at få tilmeldt sig en elektronisk tjeneste til dette - eller selv løbende at holde øje med, om der kommer nye ting til produktet. Den pågældende information bliver derfor for forbrugerne en gratis efterservice, og kunden bliver derfor bedre stillet. Yderligere kan man argumentere for, at lempelsen er meget lille, og derfor næppe vil føre til noget videre spam. Dette synspunkt finder man bl.a. hos forbrugerombudsmandens kontor: <http://www.comon.dk/index.php?page=news:print,id=14514>. Spam indeholder, som vi har set ovenfor, meget andet end reklamemails. Reklamerne er kun en del af spammails – og der er ikke noget der tyder på, at de øvrige typer vil blive påvirket af lovgivningen. Desuden viser undersøgelser, at virksomheder, som har en privacypolitik, overholder denne, og dermed ikke er kilde til spam, <http://www.cdt.org/speech/spam/030319spamreport.pdf>. Endelig kan man argumentere for, at seriøse virksomheder aldrig vil misbruge ordningen, fordi de godt ved, at de taber kunder, hvis kunderne bliver generet af at modtage for meget irrelevant information. Virksomhederne ved, at det er kunderne, der bestemmer, hvad der opfattes som spam.

Man kan klage over spam ved gennem Forbrugerstyrelsen at klage til forbrugerombudsmanden på <http://www.net-check.dk> - eller mere præcist: <http://www.net-tjek.dk/ehandel/indh1.htm>.

Sammenfatning

E-mail er en god ting, der har gjort kommunikation lettere for mange mennesker. Men effektiv anvendelse af e-mail og andre elektroniske kommunikationstjenester er truet af spam. Globalt set er ca. 50% af alle mails i dag spam. I Danmark ligger tallet på ca. 30% og det vil stige. Hvis man i fremtiden gerne vil anvende e-mails effektivt, er det derfor nødvendigt, at man overvejer at indføre adfærdsregulerende eller tekniske foranstaltninger.

De adfærdsregulerende foranstaltninger omfatter følgende punkter:

- *Der er sammenhæng mellem ledelsesansvar og it-sikkerhedspolitik*
Ledelsen har ansvaret for virksomhedens it-sikkerhedspolitik, som også bør indeholde retningslinier til, hvordan virksomheden håndterer spam-problematikken.
- *Vurder i hvilket omfang virksomheden skal beskyttes*
Virksomheden skal overveje i hvilket omfang, den vil beskytte sig, hvad og hvem den især vil beskytte sig imod og så tage de rette beslutning i overensstemmelse med virksomhedens strategi og økonomi.

- *Bør ansatte oprette en gratis webmailkonto*
Virksomheden skal overveje, hvordan den vil håndtere ansattes brug af e-mail til private formål. Herunder skal det overvejes, om medarbejderne kan tillades at læse private mails på en gratis webmail, om det kan tillades at de ansatte modtager private e-mails på virksomhedens systemer, og om virksomheden evt. vil anbefale en bestemt løsning til rådighed for medarbejdernes private brug.
- *Retningslinier for hvad folk må tilmelde sig med deres virksomhed mailkonto*
Virksomheden bør udfærdige retningslinier som specificerer, hvordan de ansatte må anvendes virksomhedens mailkonto – herunder især i forhold til anvendelse i forbindelse med nyhedsbreve og anvendelse i nyhedsgrupper. Desuden skal det anbefales medarbejderne at læse privacy politikken for nyhedsbreve, nyhedsgrupper o.s.v., hvor virksomhedens mailadresse anvendes.
- *Undlade at besvare og videresende spam*
Blandt de regler, som virksomheden bør lave, skal det fremgå, at med arbejderne ikke må besvare og videresende spammails.
- *Beskyttelse af kundekartoteker*
Virksomheden skal beskytte sine kundekartoteker således, at den ikke selv uforvarende bliver kilde til spam.
- *Opret en intern e-mail adresse til spam*
Virksomheden kan evt. oprette en mailadresse i virksomheden, hvortil de ansatte kan sende spammails.
- *Bliv ikke selv spammer*
Det er vigtigt, at man virksomheden ikke selv bliver spammer. Virksomheden bør derfor læse og følge lov om markedsføring. Virksomheden skal huske på, at det altid er kunderne, der definerer, hvad der er spam.

De tekniske foranstaltninger omfatter følgende punkter:

- *Skal virksomheden håndterer spam selv eller købe løsning hos leverandør*
Virksomheden bør tage stilling til, hvilke tekniske foranstaltninger der skal iværksættes (f.eks. aktivering af filtre i allerede indskaffet software eller indkøb af bokse til filtrering af spammails), og om disse skal styres internt eller hos en ekstern leverandør.
- *Redegøre for hvad man kan forvente sig af filtre i allerede anskaffet software og hardware*
En række af virksomhedens eksisterende produkter indeholder sandsynligvis allerede spamfiltre. Det er vigtigt at danne sig et overblik over, hvad disse kan – og at stille krav til leverandørerne ved indkøb af nyt software.
- *Spam i forbindelse med mobil opkobling*
Mobil opkobling giver virksomhederne mere fleksibilitet, men skaber i forbindelse med spam også nye problemer. Virksomheden skal tage stilling til, hvordan den vil håndtere spam i forbindelse med mobil opkobling.
- *Undlad at anvende mailadresser på hjemmesider*
Virksomheden bør i videst mulige omfang undgå at anvende mailadresser på sine hjemmesider. Dette kan undgås ved at forsøge at camouflere adressen på forskellig vis, ved at minimere antallet af adresser, ved at sørge for at mails der kommer fra henvendelse via hjemmeside har et bestemt subject/emne-felt og ved i stedet at anvende mailadresser på hjemmesiden at anvende formularer.
- *Få digital signatur*
- Virksomhedens medarbejdere bør anvende digital signatur således, at man over tid vil bidrage til sikker identifikation af afsendere. Det vil indirekte bidrage til at mængden af spam bliver mindre.

- *Skjul din e-mailadresse*
I det omfang medarbejderne har brug for at opgive mailadresser via internettet kan det være nyttigt at opgive en temporær mailadresse for at skjule sig bag ved denne. Hvis den temporære mailadresse så misbruges kan man blot nedlægge den mailadresse uden at skulle gøre noget ved den rigtige mailadresse.
- *Undlad at have open relay mailservere*
Open relay mailservere bruges til at sende spam fra. Det er derfor vigtigt at virksomheden sikrer sig, at den ikke bruger open relay og dermed bidrager til at sende spam.
- *Udform mailadresser hensigtsmæssigt*
Virksomheden bør udforme sine mailadresser hensigtsmæssigt således, at det vil blive vanskelige for en spammer at gætte sig til dem. Det betyder, at mailadresserne ikke bør laves af navne, initialer og lignende.

Links

I forbindelse med hjemmesidens oprettelse vil det blive lavet en liste med anti-spam-links.