6. It-sikkerhed

6.1. Introduktion

It-sikkerhedens betydning

Problemer med sikkerheden i netværk og computersystemer er vokset i takt med den hurtige stigning i antallet af computerbrugere. Flere og flere benytter internettet og andre netværk til at udveksle informationer. I de senere år har en række virus- og hackerangreb sat fokus på samfundets afhængighed af disse netværk og de vidtrækkende økonomiske konsekvenser, hvis systemerne ikke fungerer.

Kapitlets indhold

Kapitlet beskæftiger sig med it-sikkerhed hos virksomheder, den offentlige sektor og i befolkningen. Ved it-sikkerhed forstås både sikkerhedsproblemer og de modsvarende sikkerhedsforanstaltninger. I det følgende gives en oversigt over indholdet.

Digitale signaturer

Indledningsvis præsenteres udviklingen i udstedte certifikater til digital signatur.

It-sikkerhed i virksomheder

It-sikkerheden i virksomheder behandles, herunder forskelle i forhold til brancher og virksomhedernes størrelse. Det konstateres bl.a., at 4 ud af 5 opbevarer backup adskilt fra driftmiljøet, og at der er flest sikkerheds-foranstaltninger i de store virksomheder.

It-sikkerhed i den offentlige sektor

Under den offentlige sektor belyses it-sikkerheden i staten, amter og kommuner, herunder organisatoriske sikkerhedstiltag. Det kan fremhæves, at staten er mest udsat for Denial of service-angreb. Desuden at under halvdelen af myndighederne har en ajourført it-beredskabsplan. Endvidere kan næsten alle myndigheder nu modtage digital signatur.

It-sikkerhed i befolkningen

Befolkningens it-sikkerhed vurderes i forhold til net-handel og spam. Det ses bl.a., at bekymring for sikkerhed udgør en barriere for nethandel i befolkningen, og at yngre aldersgrupper er mere udsat for spam.

Internationalt perspektiv

Danske virksomheder ligger over EU-gennemsnittet mht. it-sikkerhedsforanstaltninger (afsnit 6.6.).

6.2 Digital signatur

Mærkbar stigning i udbredelsen af digital signatur

Antallet af udstedte certifikater til digital signatur er steget markant (figur 6.1). Efter en beskeden start i 1. halvår af 2003 tog udviklingen fart i 2. halvår med en fortsat stigning i 2004, 2005 og 2006. Ved udgangen af september 2006 var der udstedt i alt 720.000 certifikater til digitale signaturer.

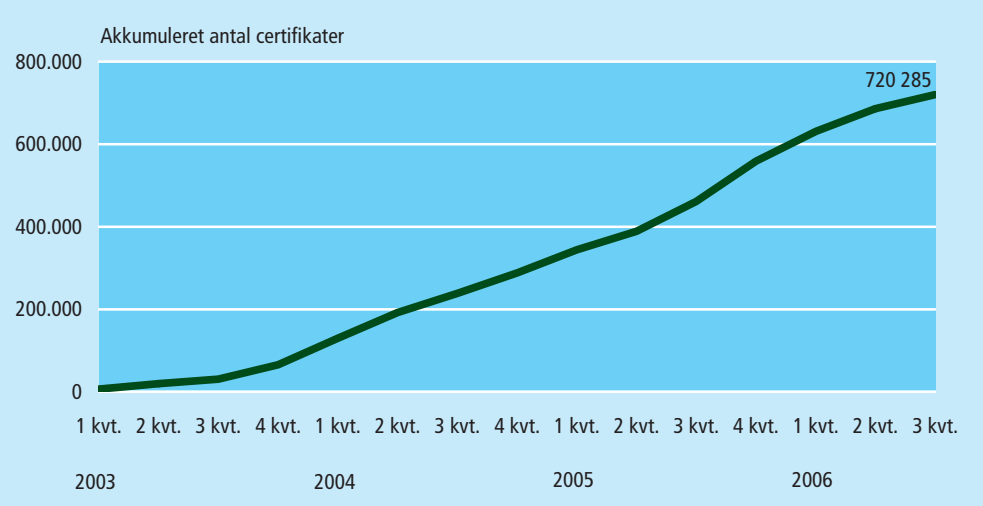
Antallet svarer til hver femte dansker i alderen 16-74 år

Sat i forhold til den danske befolkning i alderen 16-74 år svarer det til ca. 20 pct. - her skal dog tages forbehold for at et antal danskere har såvel en privat- som medarbejdersignatur, så andelen af brugere alt andet lige vil ligge lavere.

Certifikater til private og medarbejdere

Der er både tale om certifikater til private og medarbejdercertifikater. Det vil sige enkeltpersoners eller medarbejderes mulighed for at kommunikere sikkert med internetbaserede services - herunder bl.a. Skats TastSelv, sundhed.dk, e-boks mv.

Figur 6.1 **Antal udstedte certifikater til digital signatur**



Anm. Estimater på baggrund af ugentlige tal.
Kilde: TDC, 2006.

Om digitale signaturer

Antallet af udstedte certifikater indikerer hvor mange borgere og medarbejdere, der er i stand til at anvende digital signatur, fx i kommunikation med virksomheder og myndigheder. Det samlede antal certifikater på 720.285 fordeler sig på 607.429 personcertifikater og 112.856 medarbejdercertifikater.

Virksomhedscertifikater er ikke medtaget i disse tal. Borgere, der har flere private signaturer tæller kun med én gang i figur 6.1. Mht. medarbejdercertifikater, kan en medarbejder have mere end én signatur.

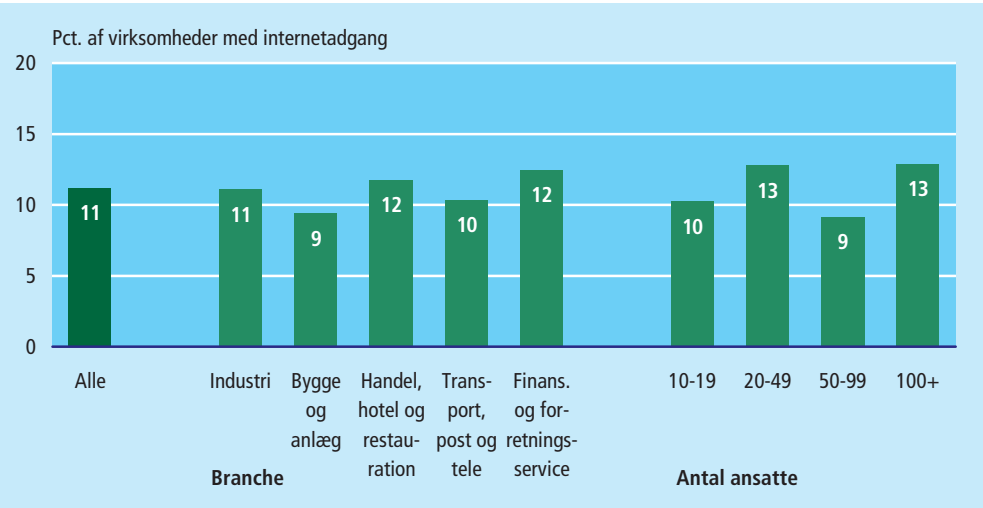
6.3 It-sikkerhed i virksomhederne

It-sikkerhedsproblemer

It-sikkerhedsproblem med tab af data eller arbejdstid

Lidt over hver tiende virksomhed havde et it-sikkerhedsproblem i løbet af 2005, fx i form af et virusangreb, som medførte tab af data eller arbejdstid (figur 6.2). Der er i almindelighed ingen markante forskelle mellem branche- og størrelsesgrupper.

Figur 6.2 **Virksomhedernes it-sikkerhedsproblemer med tab af data eller arbejdstid. 2005**



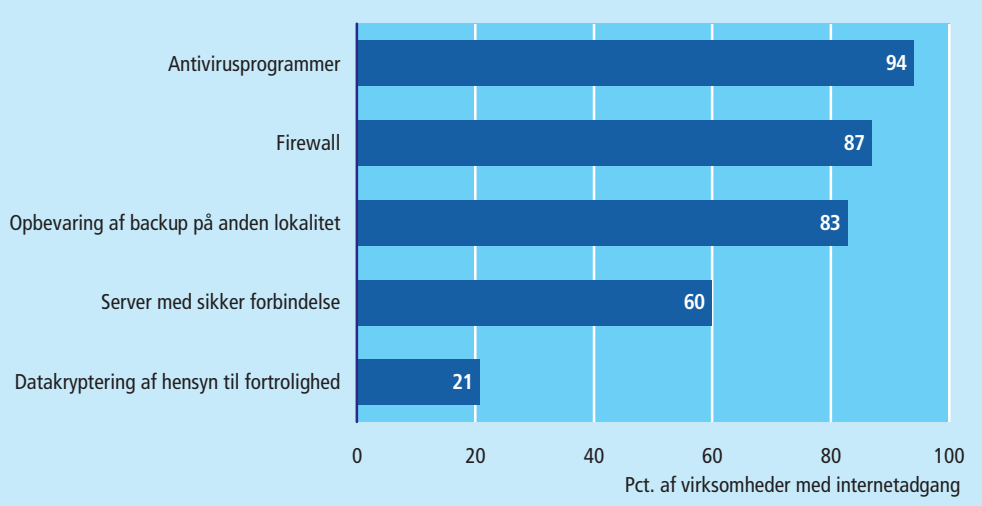
Anm.: Virksomheder med internetadgang blev spurgt: "Har virksomheden været udsat for it-sikkerhedsproblemer med tab af data eller arbejdstid i 2005 (fx virusangreb eller uautoriseret adgang til systemer eller data)?".
Årets tal kan ikke umiddelbart sammenlignes med tidligere år, idet spørgsmålet er ændret.
Kilde: Danmarks Statistik, Danske virksomheders brug af it 2006.

It-sikkerhedsforanstaltninger

4 ud af 5 opbevarer backup adskilt fra driftmiljøet

Antivirusprogrammer findes hos 94 pct. af alle virksomheder med internetadgang, og er dermed den hyppigste it-sikkerhedsforanstaltning (figur 6.3). 87 pct. anvender firewall og 83 pct. opbevarer backup på anden lokalitet end driftmiljøet. 60 pct. har en server med sikker forbindelse (som understøtter sikkerhedsprotokoller, fx SSL eller SHTTP). Endelig anvender 21 pct. datakryptering af hensyn til fortrolighed.

Figur 6.3 **Virksomhedernes it-sikkerhedsforanstaltninger. 2006**



Kilde: Danmarks Statistik, Danske virksomheders brug af it 2006.

Flest sikkerheds-foranstaltninger i de store virksomheder

It-sikkerhedsforanstaltninger er generelt lidt mere udbredt blandt de større virksomheder. Det drejer sig især om foranstaltninger som server med sikker forbindelse samt brug af datakryptering (tabel 6.1).

Tabel 6.1 **Virksomhedernes it-sikkerhedsforanstaltninger. 2006**

	Alle virksomheder	Antal ansatte	
		10-49	50+
	pct. af virksomheder med internetadgang		
Antivirusprogrammer	94	93	99
Firewall	87	84	98
Opbevaring af backup på anden lokalitet	83	81	93
Server med sikker forbindelse[1]	60	56	78
Datakryptering af hensyn til fortrolighed	21	16	40

[1] Som understøtter sikkerhedsprotokoller, fx SSL eller SHTTP.

Kilde: Danmarks Statistik, Danske virksomheders brug af it 2006.

Generelt ensartet niveau for it-sikkerhed i regionerne

Der er ingen stor forskel mellem regionerne, hvad angår de mest almindelige sikkerhedsforanstaltninger som antivirusprogrammer, firewall samt opbevaring af backup på anden lokalitet end driftmiljøet (tabel 6.2).

Flest virksomheder i hovedstaden bruger datakryptering og server med sikker forbindelse

Mht. server med sikker forbindelse ligger hovedstadsregionen noget over gennemsnittet, Midtjylland på gennemsnittet og de tre øvrige regioner lidt under. Denne regionale forskel er også gældende, hvad angår datakryptering, som anvendes af 29 pct. af virksomhederne i hovedstadsregionen mod 15-19 pct. i de øvrige fire regioner.

Tabel 6.2 **Virksomhedernes it-sikkerhedsforanstaltninger, regionalt fordelt. 2006**

	Hele landet	Hoved-staden	Sjælland	Syd-danmark	Midt-jylland	Nord-jylland
	pct. af virksomheder med internetadgang					
Antivirusprogrammer	94	96	90	93	96	92
Firewall	87	91	85	85	87	83
Opbevaring af backup på anden lokalitet	83	83	80	84	82	84
Server med sikker forbindelse[1]	60	67	57	55	60	55
Datakryptering af hensyn til fortrolighed	21	29	15	16	19	17

[1] Som understøtter sikkerhedsprotokoller, fx SSL eller SHTTP.

Anm.: Tal på regionalt niveau er forbundet med noget større statistisk usikkerhed end tal for hele landet.

Kilde: Danmarks Statistik, Danske virksomheders brug af it 2006.

6.4 It-sikkerhed i den offentlige sektor

It-sikkerhedsproblemer

Fald i virusangreb med tab af data eller arbejdstid

3 ud af 10 myndigheder i stat og kommuner og 8 ud af 10 amter havde inden for det seneste år oplevet virusangreb med tab af data eller arbejdstid af genererende eller alvorlig karakter (tabel 6.3). Der er tale om et klart fald fra 43 pct. i 2004.

Staten mest udsat for Denial of Service-angreb

Denial of Service-angreb har fundet sted hos 17 pct. af alle myndigheder; igen hyppigere hos amterne (55 pct.) end i staten og hos kommunerne (13 pct. og 16 pct.). Denial of Service-angreb er et forsøg på at forstyrre eller stoppe kommunikationen til et netværk ved at fremsende overflødige data.

Datatab pga. manglende backup sjældent i kommunerne

Datatab pga. manglende backup fandt sted hos omkring hver tiende myndighed, dog mere end dobbelt så hyppigt i staten og amterne end hos kommunerne. Uautoriseret adgang til systemer og data fandt sted hos 13 pct. i staten, hos 36 pct. af amterne og 7 pct. af kommunerne.

Økonomisk misbrug og afpresning er sjældent

Endelig blev der spurgt til it-misbrug af økonomisk karakter (fx bedrageri) og afpresning/trusler rettet mod data eller software. Disse to sikkerhedsproblemer er generelt ikke tilstede blandt myndighederne.

Tabel 6.3 **Myndigheder der havde været udsat for problemer i forhold til it-sikkerhed. 2005**

	I alt	Stat	Amter	Kommuner		
				I alt	Under 15.000 indb.	Mindst 15.000 indb.
	pct.					
Virusangreb med tab af data/arbejdstid	31	32	82	28	30	23
Denial of Service-angreb[1]	17	13	55	16	14	22
Datatab pga. manglende backup	11	18	18	7	7	6
Uautoriseret adgang til systemer og data	10	13	36	7	6	11
Økonomisk it-misbrug	1	1	9	1	0	2
Afpresning/trusler mod data el. software	1	0	0	1	1	2

Anm.: Spørgsmålet lød: "Har myndigheden været udsat for nogle af følgende problemer inden for det seneste år?" Procenterne angiver andelen, hvor problemet blev betegnet som 'alvorligt' eller 'generende'. Ingen benyttede sig af svarmuligheden 'katastrofal' betydning, hvorfor denne kategori er slået sammen med 'alvorligt'.

[1] Denial of Service-angreb er et forsøg på at forstyrre eller stoppe kommunikationen til et netværk ved at fremsende overflødige data.

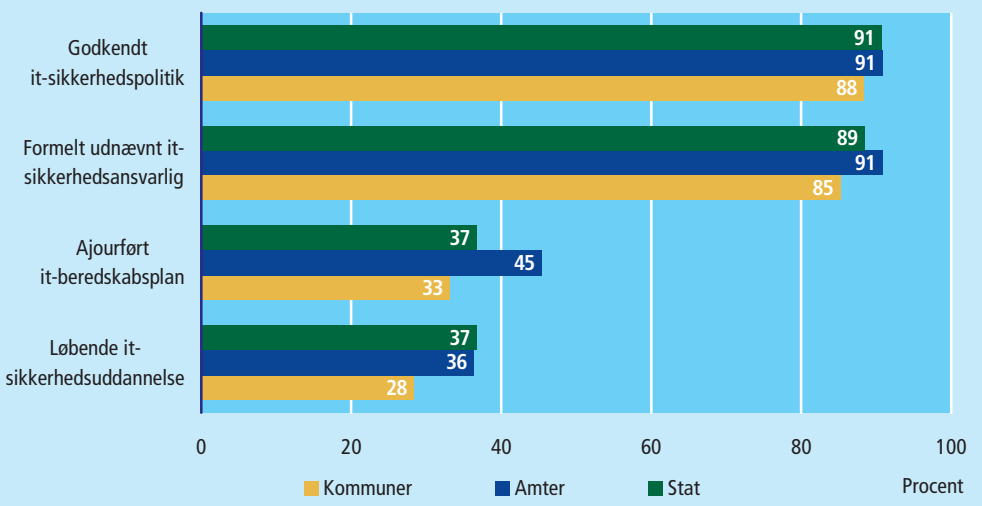
Kilde: Danmarks Statistik, Den offentlige sektors brug af it 2005.

It-sikkerhedsforanstaltninger

Under halvdelen af myndighederne har en ajourført it-beredskabsplan

It-sikkerhedspolitik, som er godkendt af ledelsen, findes hos omtrent 9 ud af 10 myndigheder og er dermed det mest udbredte organisatoriske sikkerhedstiltag (figur 6.4). En næsten lige så stor andel af myndighederne har formelt udnævnt en it-sikkerhedsansvarlig. Hver tredje kommune har en it-beredskabsplan, som er ajourført inden for de seneste to år, og lidt flere blandt amter og statslige myndigheder. Næsten samme udbredelse gør sig gældende mht. løbende it-sikkerhedsuddannelse af medarbejdere.

Figur 6.4 **Organisatoriske sikkerhedstiltag i den offentlige sektor. 2005**

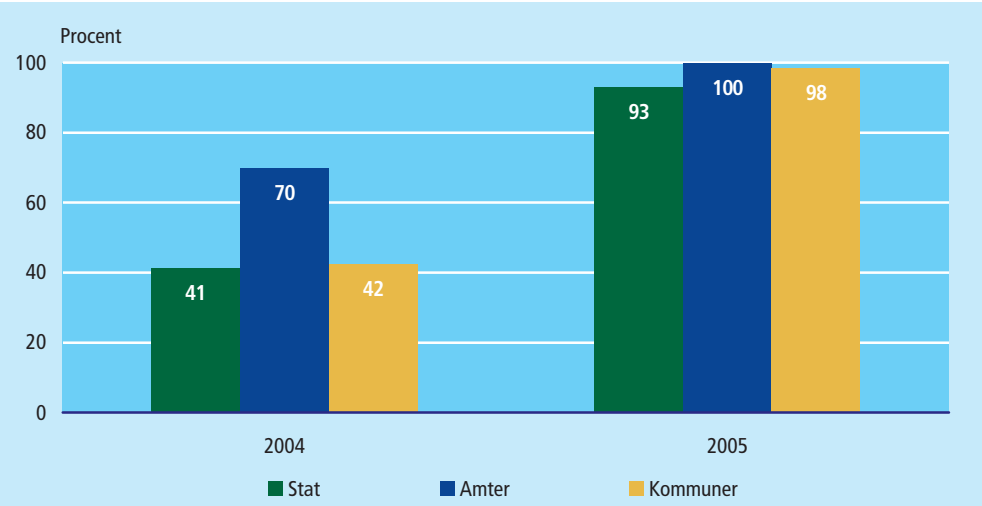


Kilde: Danmarks Statistik, Den offentlige sektors brug af it 2005.

Næsten alle myndigheder kan modtage digital signatur

Andelen af myndigheder, der kan modtage digital signatur er mere end fordoblet fra 2004 til 2005 (figur 6.5). Myndighedernes tjenester til digital signatur kan være i form af løsninger for sikker signeret e-post, log-on på hjemmeside eller for udfyldte blanketter. Hvor 4 ud af 10 myndigheder i stat og kommuner og 7 ud af 10 amter kunne modtage digital signatur i 2004, var det tæt på alle myndigheder i 2005.

Figur 6.5 **Myndigheder der modtager digital signatur[1]. 2004-2005**



Anm.: Ved digital signatur forstås den fælles offentlige OCES-standard (Offentlige Certifikater til Elektronisk Service), der muliggør elektronisk identifikation, underskrift og kryptering.

[1] Enten som 'modtagelse af signeret e-post', 'log-on på hjemmeside via digital signatur' eller 'udfylde og underskrive/verificere blanketter'. Tal vedr. 2004 er eksklusive 'udfylde og underskrive/verificere blanketter', men dette har imidlertid ingen væsentlig betydning for det samlede niveau i 2005.

Kilde: Danmarks Statistik, Den offentlige sektors brug af it 2004 og 2005.

Parat til eDag2

Udviklingen i tallene er formentlig en virkning af den såkaldte eDag2 pr. 1. februar 2005 - fra denne dag har alle offentlige myndigheder i stat, amt og kommune som udgangspunkt ret til at sende breve og dokumenter med følsomme og fortrolige oplysninger fuldt elektronisk til andre myndigheder. Tilsvarende kan de forlange, at andre myndigheder sender fuldt elektronisk til dem. Endvidere har borgere og virksomheder ret til at sende sikker elektronisk post til det offentlige. Tallene afspejler myndighedernes parathed på området, men derimod ikke udnyttelsesgraden.

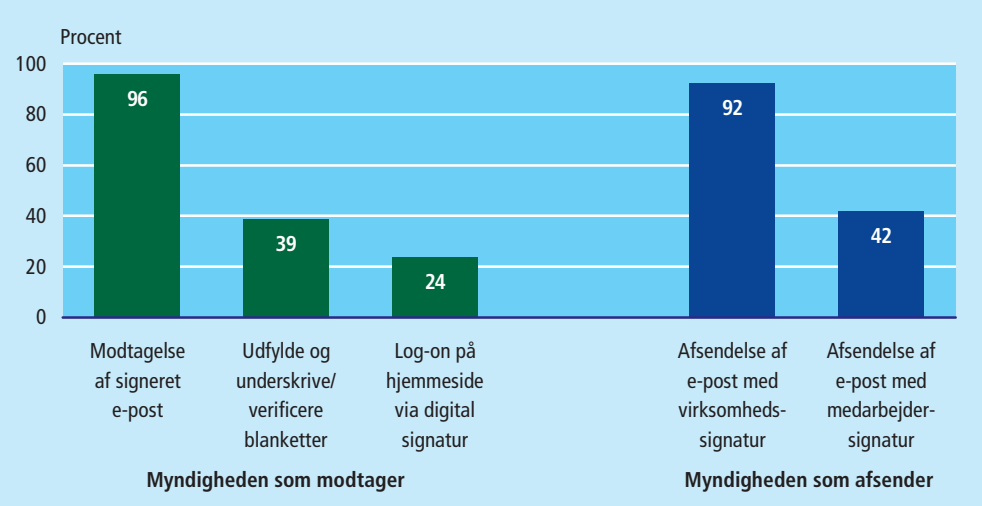
Digital signatur via e-post mest udbredt

Den mest udbredte løsning mht. digital signatur er muligheden for at modtage og afsende sikker e-post, hvilket stort set svarer til andelen af myndigheder med digital signatur i alt (figur 6.6). Næsten 4 ud af 10 myndigheder har digitale blanketter, som kan udfyldes og underskrives med digital signatur. Endelig har lidt under hver fjerde myndighed en log-on-facilitet på hjemmesiden, som baserer sig på digital signatur.

Næsten alle kan afsende e-post med digital signatur

92 pct. af myndighederne kan afsende e-post med digital virksomhedssignatur og 42 pct. kan afsende med medarbejdersignatur. Næsten alle - 97 pct. - kan afsende e-post med en af de to varianter.

Figur 6.6 **Anvendelse af digital signatur. 2005**



Kilde: Danmarks Statistik, Den offentlige sektors brug af it 2005.

Kommuner har den bredeste brug af digital signatur

Der er ikke den store forskel på myndighederne mht. brug af digital signatur i forbindelse med e-post. Til gengæld ligger kommunerne en del foran stat og amter mht. brug af digital signatur til at underskrive blanketter samt ved log-on på hjemmeside (tabel 6.4).

Sikre forbindelser især udbredt blandt de større kommuner

Blandt andre foranstaltninger til sikker kommunikation kan nævnes 'sikker forbindelse' samt log-on via adgangskode (fx pinkode). Sikker forbindelse findes hos lidt mere end hver tredje myndighed; hyppigst hos de større kommuner med mindst 15.000 indbyggere. Log-on på hjemmesiden via adgangskode findes hos næsten 4 ud af 10 myndigheder i staten, i under 3 ud af 10 blandt amter og under hver fjerde myndighed i kommunerne (23 pct.).

Tabel 6.4 **Sikker kommunikation med myndigheder. 2005**

	I alt	Stat	Amter	Kommuner		
				I alt	Under 15.000 indb.	Mindst 15.000 indb.
	pct.					
Digital signatur (myndigheden som modtager)	**97**	**93**	**100**	**98**	**98**	**100**
Modtagelse af signeret e-post	96	92	100	97	97	98
Udfylde og underskrive/verificere blanketter	39	10	18	53	50	60
Log-on på hjemmeside via digital signatur	24	18	9	27	23	35
Digital signatur (myndigheden som afsender)	**97**	**94**	**100**	**97**	**97**	**98**
Afsendelse af e-post med virksomhedssignatur	92	84	100	96	94	98
Afsendelse af e-post med medarbejdersignatur	42	40	45	43	41	46
Andre former for sikker kommunikation						
Sikker forbindelse (understøttet af servercertifikater[1])	35	34	27	35	27	51
Log-on - via pinkode eller adgangskode	28	39	27	23	18	31

Anm.: Ved digital signatur forstås den fælles offentlige OCES-standard (Offentlige Certifikater til Elektronisk Service), der muliggør elektronisk identifikation, underskrift og kryptering.
[1] Server-certifikater bruges bl.a. til at dokumentere hjemmesidens ægthed over for brugere og til at kryptere kommunikation mellem brugere og myndighed.
Kilde: Danmarks Statistik, Den offentlige sektors brug af it 2005.

6.5 It-sikkerhed i befolkningen

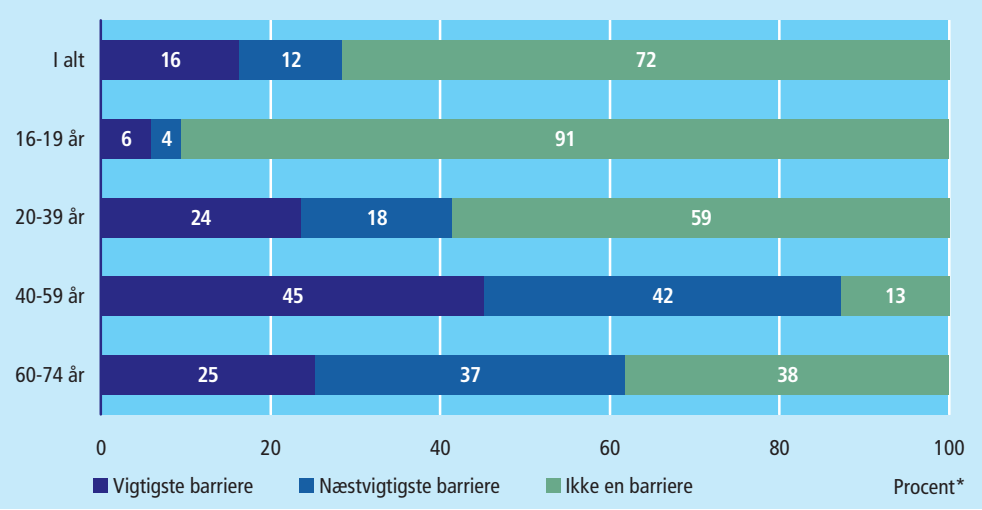
Bekymring for sikkerhed barriere for nethandel ...

Blandt den del af befolkningen der har anvendt internettet, men som ikke har e-handlet i de seneste 12 måneder, er bekymring for sikkerheden ved betaling den største eller næststørste barriere for internetkøb hos 28 pct. (figur 6.7). Det er kun overgået af barrieren 'har ikke brug for internet-handel' (45 pct.) samt ønsket om at 'se varen inden køb/butiksloyalitet' (41 pct.).

... især blandt 40-49-årige

Der er imidlertid en del forskel på aldersgrupperne. Således topper bekymringen for manglende sikkerhed ved betaling i aldersgruppen 40-59 år, hvor hele 87 pct. har dette som vigtigste eller næstvigtigste barriere for køb via internettet. I aldersgruppen 20-39 år er andelen 42 pct., og blandt 16-19-årige, der ikke har e-handlet i de seneste 12 måneder, er det kun hver tiende, der har manglende betalingssikkerhed som vigtigste eller næstvigtigste barriere.

Figur 6.7 **Barrierer for køb via internettet - bekymret for sikkerheden ved betaling. 2006**



* Procentgrundlag: Pct. af dem der har anvendt internettet, men ikke har e-handlet i de seneste 12 måneder.
Kilde: Danmarks Statistik, Befolkningens brug af internet 2006.

59 pct. af daglige internetbrugere har modtaget spam

Hyppige internetbrugere er mere udsat for spam end de, der sjældnere bruger internettet (figur 6.8). Blandt daglige brugere har 59 pct. modtaget spam inden for den seneste måned mod 37 pct. blandt de ugentlige brugere og 17 pct. blandt månedlige brugere.

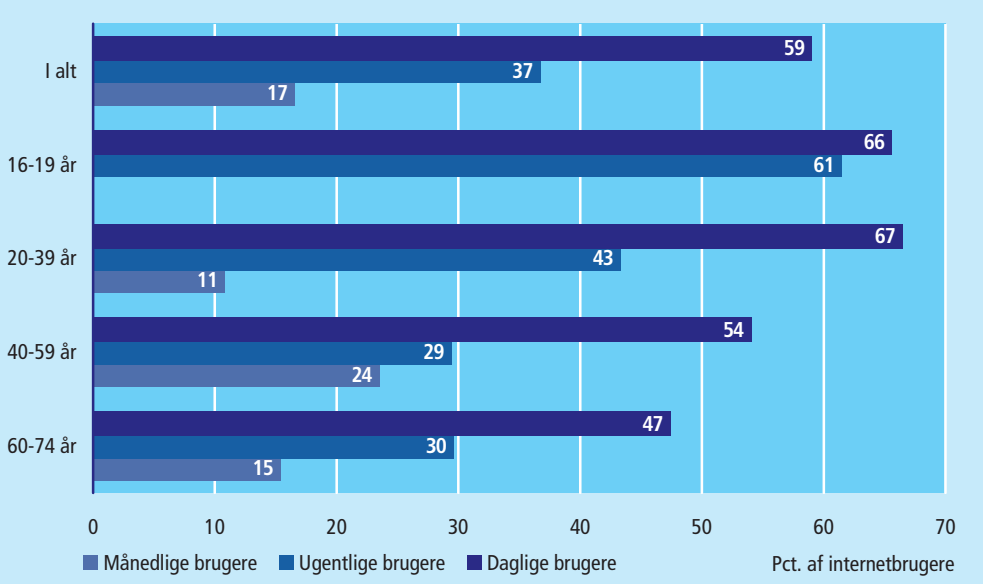
Yngre aldersgrupper mere udsat for spam

De yngre aldersgrupper er generelt mere udsat for spam end de ældre aldersgrupper. Det er de først og fremmest pga. en hyppigere brug af internettet, men tallene viser også, at blandt de daglige brugere er de yngre aldersgrupper under 40 år mere udsatte end de på mindst 40 år. Ser man på de ugentlige brugere er forskellen endnu større mellem aldersgrupperne.

Forbrugsmønster kan give spam

Yngre personer synes således at være mere udsatte for spam end de ældre personer, også når der tages højde for forskel i brugshyppigheden af internettet. Forskellen mellem aldersgruppernes modtagelse af spam kan tænkes også at hænge sammen med et andet forbrugsmønster hos de yngre internetbrugere, herunder større brug af internettjenester og kommunikation, som i højere grad forbindes med spam.

Figur 6.8 **Spam modtaget i den sidste måned blandt internetbrugere. 2006**



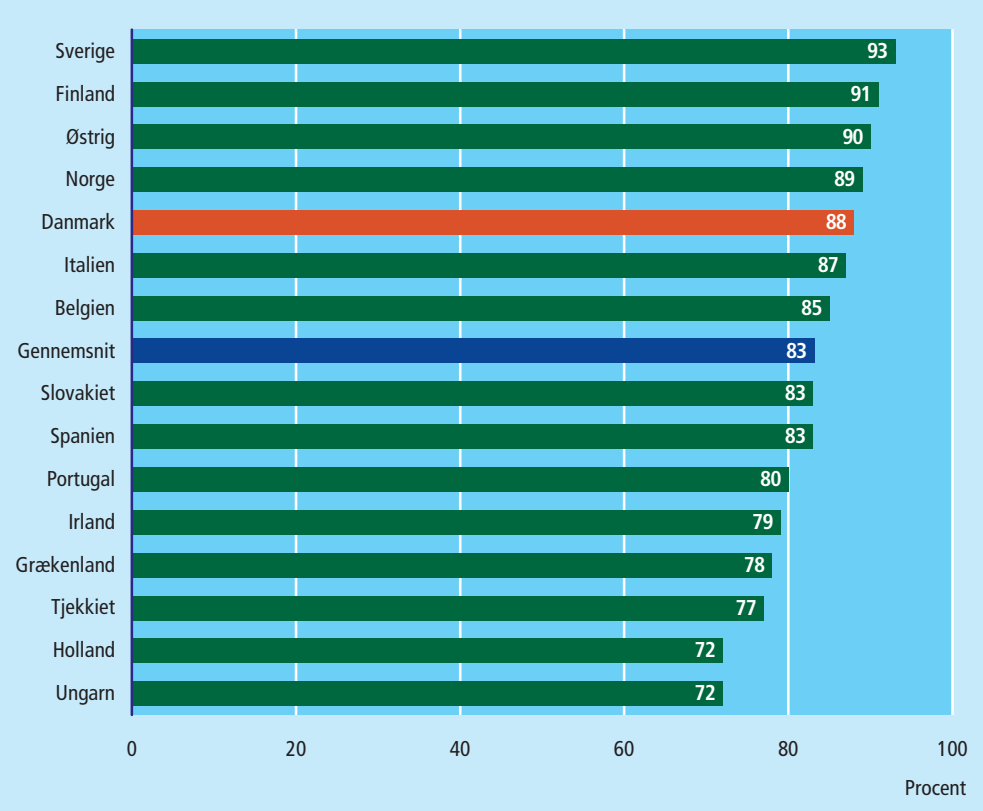
Anm.: Antallet af 16-19-årige månedlige internetbrugere er så lille i undersøgelsen, at andelen af spammodtagere ikke kan opgøres med sikkerhed.
Kilde: Danmarks Statistik, Befolkningens brug af internet 2006.

6.6 Internationalt perspektiv

Danske virksomheders it-sikkerhed over gennemsnittet

Det store flertal af europæiske virksomheder i en række EU-lande har opdateret deres it-sikkerhedsforanstaltninger inden for de seneste 3 måneder (figur 6.9). Blandt danske virksomheder ligger andelen på 80 pct., hvilket bringer Danmark på en femteplads. Længst fremme ligger Sverige med 93 pct., fulgt af Finland, Østrig og Norge.

Figur 6.9 **Virksomheder med opdaterede it-sikkerhedsforanstaltninger[1]. 2005**



Anm. Figuren viser 15 udvalgte EU-lande. De nordiske lande indgår så vidt muligt. Derudover er de 10 bedst placerede lande udvalgt blandt de 15 største lande ud over Norden.

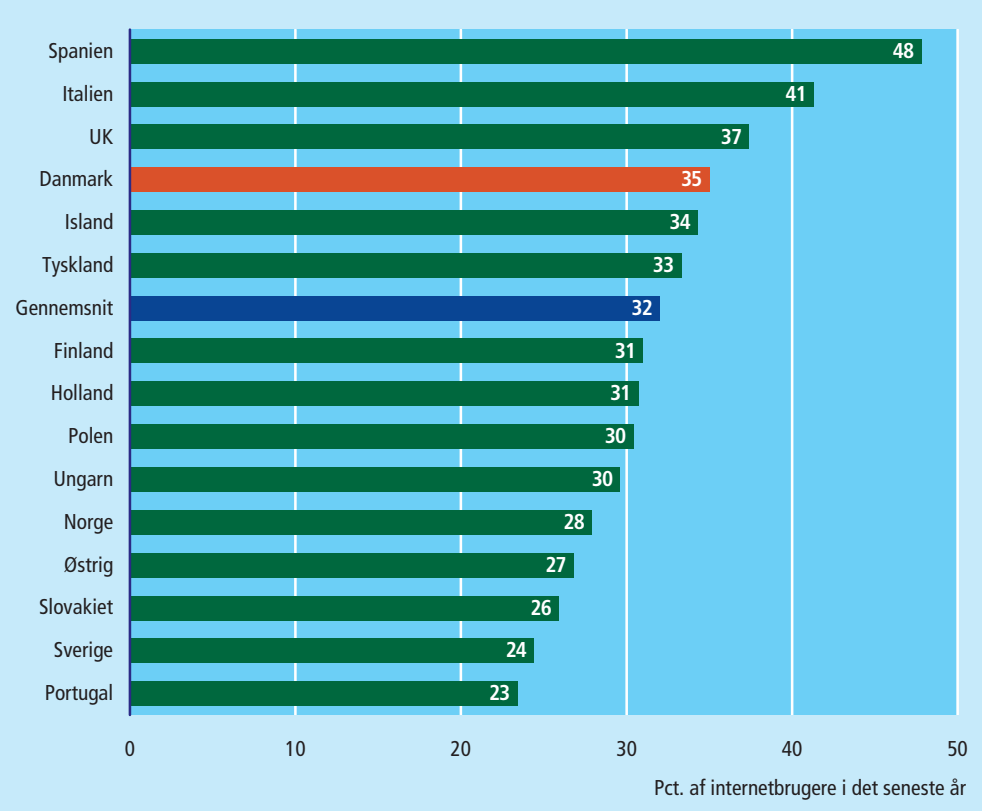
[1] Mindst én foranstaltning, som er opdateret inden for de seneste tre måneder (fx automatisk opdatering af antivirus-programmer).

Kilde: Eurostat, februar 2005 (http://europa.eu.int/comm/eurostat/). Islandske data er fra 2003-undersøgelsen.

Danske borgere mere udsat for virusangreb

35 pct. af danske internetbrugere har været udsat for et virusangreb med tab af information eller tid, hvilket er lidt over gennemsnittet af en række EU-lande (figur 6.10). Typisk vil hyppige brugere af internettet være mere udsat for virusangreb, men en lang række andre årsager kan spille ind i forhold til de nationale forskelle.

Figur 6.10 **Borgere udsat for virusangreb[1]. 2005**



Anm.: Figuren viser 15 udvalgte EU-lande. De nordiske lande indgår så vidt muligt. Derudover er de 10 højest placerede lande udvalgt blandt de 15 største lande ud over Norden.

[1] Computervirus som inden for de seneste 12 måneder har forårsaget tab af information eller tid.

Kilde: Eurostat, oktober 2006 (http://europa.eu.int/comm/eurostat/).