Mads Hansen-Møllerud, Geir Martin Pilskog og Anne-Hege Sølverud

7. Sikkerhet

Vanskeligheter med sikkerheten på Internett og andre nettverk vokser med økende bruk av informasjons- og kommunikasjonsteknologi (IKT). Faren for at informasjon blir endret, går tapt eller blir stjålet er en av de uheldige følgene av den store utbredelsen av Internett. Manglende sikkerhet er en viktig barriere for utviklingen av et elektronisk tjenestetilbud. Sikkerhetsproblemer kan medføre økonomisk tap eller redusert tillit og anseelse. Blant annet virusangrep har satt fokus på sårbarhet knyttet til IKT på forskjellige samfunnsområder.

Regjeringen har i dokumentet "Nasjonal strategi for informasjonssikkerhet" (juni 2003) skissert fire overordnede mål for informasjonssikkerhet i det norske samfunnet:

- Samfunnskritisk infrastruktur for elektronisk informasjonsutveksling skal være robust og sikker i forhold til de trusler den utsettes for. Kritiske informasjonssystemer skal være sikret slik at skadevirkningene ved sikkerhetsbrudd ikke er større enn hva som kan defineres som akseptabel risiko.
- Det skal bygges en sikkerhetskultur rundt bruk og utvikling av informasjonssystemer og elektronisk informasjonsutveksling i Norge. IT-sikkerhet skal være en sentral faktor ved forbrukernes og norske virksomheters bruk av IT.
- Norge skal ha en allment tilgjengelig samfunnsinfrastruktur for elektronisk signatur, autentisering av kommunikasjonspartnere samt sikker overføring av sensitiv informasjon.
- Regelverk som berører informasjonssikkerhet, skal håndheves og videreutvikles på en samordnet, og for brukere enkel og oversiktlig måte, slik at gjennomføringen av nødvendige tiltak skjer på en mest mulig effektiv og samtidig forsvarlig måte.

Det er ikke en naturlig oppgave for Statistisk sentralbyrå å vurdere håndhevingen av regelverket for informasjonssikkerhet. Dette kapitlet inneholder informasjon om bruk av digital signatur og IKT-sikkerhet i næringslivet, offentlig sektor og husholdningene. Både data om sikkerhetsproblemer og -tiltak presenteres. Forholdene i Norge blir sammenlignet med andre land, og noen av variablene blir også fordelt regionalt.

7.1. Digital signatur

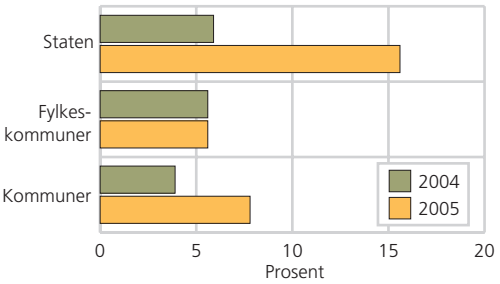
Avsnittet presenterer informasjon om bruk av digital signatur i næringslivet og offentlig sektor. Digital signatur brukes for å sikre utveksling av informasjon mellom to parter. Når en person, et IT-system eller en server sender en melding eller et dokument til en mottaker, kan dokumentet signeres med en spesiell kode (basert på privat nøkkel fra avsenders sertifikat) som bare riktig avsender har tilgang til. Ut fra signaturen på forsendelsen kan mottaker verifisere hvem som faktisk har sendt dokumentet. Signaturen kan også brukes for å avgjøre om selve innholdet i dokumentet har blitt endret på veien fra avsender til mottaker.

- Bruk av digital signatur økte blant statlige foretak fra 2004 til 2005. Blant kommuner og fylkeskommuner var det små eller ingen forandringer i denne perioden.
- Bruk av digital signatur var lite utbredt i næringslivet i 2005.

Bruk av digital signatur i offentlig sektor

- Andelen statlige foretak, fylkeskommuner og kommuner som benyttet digital signatur ved kommunikasjon over Internett var på henholdsvis 6, 6 og 4 prosent i 2004. I 2005 hadde disse andelene steget til 16 prosent blant statlige foretak og 8 prosent blant kommunene. For fylkeskommunene ble det ikke registrert noen endring.

Figur 7.1.1. Andel kommuner, fylkeskommuner og statlige foretak som kommuniserer ved hjelp av digital signatur. 2004 og 2005. Prosent

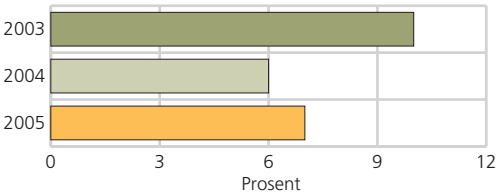


Kilde: Statistisk sentralbyrå.

Bruk av digital signatur i næringslivet

- Bruk av digital signatur er lite utbredt i næringslivet. Foretakene ble bedt om å rapportere om det var mulig å kommunisere med dem ved hjelp av "Digital signatur (som mottaker)". I 2005 bekreftet 7 prosent at de brukte digital signatur, mot 6 prosent i 2004.

Figur 7.1.2. Andel av alle foretak som kommuniserte med digital signatur. Foretak med 10+ sysselsatte. 2003-2005. Prosent



Kilde: Statistisk sentralbyrå.

Om statistikken

Datagrunnlaget for offentlig sektor er hentet fra Statistisk sentralbyrås undersøkelser om bruk av IKT i henholdsvis kommunene, fylkeskommunene og staten. Alle undersøkelsene er fulltellinger og staten er definert som alle foretak innenfor stats- og trygdeforvaltningen, statens forretningsdrift, statlige låneinstitusjoner, statsforetak (100 prosent eid av staten) samt Norges Bank. Oslo inngår i kommunetallene og ikke i fylkestallene. Ytterligere detaljer om undersøkelsene er beskrevet i kapittel 6.

Datagrunnlaget for næringslivet er hentet fra samme statistikk som blir beskrevet i avsnitt 7.2.

Internett-referanser: www.ssb.no/iktbrukn/
www.ssb.no/iktbrukk/
www.ssb.no/iktbruks/

Tabell 7.1.1. Andel kommuner, fylkeskommuner og statlige foretak som kommuniserer ved hjelp av digital signatur. 2004 og 2005. Prosent

	Andel kommuner	Andel fylkeskommuner	Andel statlige foretak
2004	4	6	6
2005	8	6	16

Kilde: Statistisk sentralbyrå.

Tabell 7.1.2. Andel av alle foretak som kommuniserte ved hjelp av ulike sikkerhetstiltak. Alle foretak med 10+ sysselsatte. 2003-2005. Prosent

Sikkerhetstiltak	2003	2004	2005
Digital signatur	10	6	7
Andre metoder til indentifikasjon enn digital signatur, f.eks. PIN-kode	13	10	13
Kryptering av hensyn til konfidensialitet	8	7	11

Kilde: Statistisk sentralbyrå.

7.2. IKT-sikkerhet i næringslivet

Avsnittet presenterer noen sikkerhetsproblem i næringslivet i tidsrommet 2003-2005. Videre inneholder avsnittet informasjon om næringslivets sikkerhetstiltak i samme perioden.

- Virusangrep er et av de mest vanlige sikkerhetsproblemene i næringslivet, men omfanget av problemet har minket siden 2003.
- Nesten alle foretak benytter beskyttelsesprogramvare. I 2005 brukte nesten 90 prosent viruskontroll/beskyttelsesprogramvare, mot vel 80 prosent i 2003.

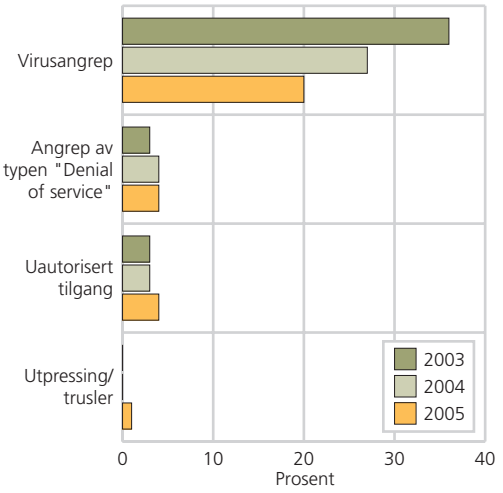
Virusangrep er et vanlig problem

- Virusangrep er et vanlig sikkerhetsproblem i næringslivet. To av ti foretak opplevde virusangrep i 2005. Resultatet er en nedgang i forhold til 2003 og 2004, da henholdsvis 36 og 27 prosent ble utsatt for problemet.
- 1 prosent av foretakene meldte om utpressing/trusler mot foretakets data eller programvare i 2005. Selv om fenomenet er lite utbredt, skyldes en så liten andel også uvilje mot å vedgå problem i eget foretak.

Nesten alle bruker viruskontroll

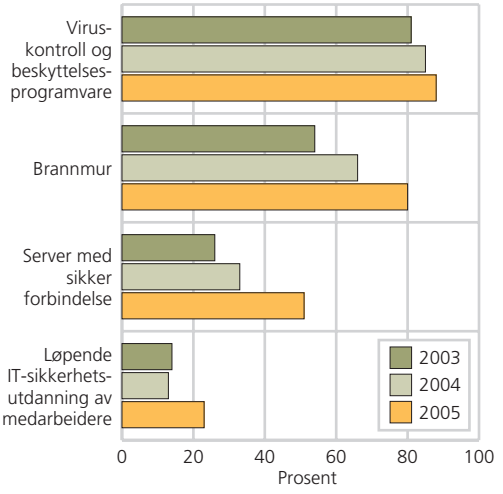
- Næringslivet prøver å beskytte seg mot ulike former for sabotasje. Programvare mot virus er det mest brukte sikkerhetstiltaket. Knapt 90 prosent av foretakene benyttet beskyttelsesprogramvare i 2005.
- Det var en økning i andelen foretak med løpende sikkerhetsutdanning av medarbeidere. I 2005 sørget nesten en firedel av foretakene for å oppdatere kunnskapen til medarbeiderne om sikkerhetsproblem. I 2004 var den tilsvarende andelen 13 prosent.

Figur 7.2.1. Andel av alle foretak med utvalgte sikkerhetsproblemer. Foretak med 10+ sysselsatte. 2003-2005. Prosent



Kilde: Statistisk sentralbyrå.

Figur 7.2.2. Andel av alle foretak med utvalgte sikkerhetstiltak. Foretak med 10+ sysselsatte. 2003-2005. Prosent



Kilde: Statistisk sentralbyrå.

Om statistikken

Datagrunnlaget er hentet fra Statistisk sentralbyrås utvalgsundersøkelser av bruk av IKT i næringslivet. De omfattet primært foretak med minst ti sysselsatte, men det ble også trukket et tilleggsutvalg for foretak med under ti sysselsatte. Populasjonen for undersøkelsen omfatter alle næringsområder utenom primærnæringene, bergverksdrift, offentlig administrasjon, kloakk og renovasjon, interesseorganisasjoner, lønnet arbeid i private husholdninger og internasjonale organ og organisasjoner. Utvalget inneholder knapt 5 000 foretak og svarprosenten ligger på om lag 75.

Internett-referanse: www.ssb.no/iktbrukn/

Tabell 7.2.1. Andel av alle foretak utsatt for ulike sikkerhetsproblemer seneste året. Alle foretak med 10+ sysselsatte. 2003-2005. Prosent

Sikkerhetsproblem	2003	2004	2005
Sabotasje	1	1	2
IT-misbruk av økonomisk karakter	1	1	2
Utpressing/trusler mot data/programvare	0	0	1
Uautorisert tilgang til system/data	3	3	4
Angrep av typen "Denial of service"	3	4	4
Datatap pga. manglende backup	8	7	7
Maskinvarefeil	33	35	42
Programvarefeil	36	36	44
Virusangrep	36	27	20
Sammenbrudd i forbindelsen til Internett eller andre eksterne nettverk	28	28	32
Tyveri av datautstyr som kan bæres	:	9	11

Kilde: Statistisk sentralbyrå.

Tabell 7.2.2. Andel av alle foretak som brukte ulike sikkerhetstiltak. Alle foretak med 10+ sysselsatte. 2003-2005. Prosent

Sikkerhetstiltak	2003	2004	2005
Fysisk adgangsbegrensning til kritisk IT-utstyr	31	36	49
Nødstrømsanlegg	38	36	46
Oppbevaring av backup på annen lokalitet enn driftsmiljøet	63	61	68
Server med sikker forbindelse (understøtter sikkerhetsprotokoller, f.eks. SSL eller SHTTP)	26	33	51
Brannmur	54	66	80
Viruskontroll og beskyttelsesprogramvare	81	85	88
Løpende abonnement på sikkerhetsservice (f.eks. antivirusprogram eller program som varsler angrep)	57	68	82
Løpende IT-sikkerhetsutdannelse av medarbeidere	14	13	23
IT-sikkerhetspolitikk godkjent av ledelsen	:	23	46
Formelt utnevnt IT-sikkerhetsansvarlig	:	28	39
Kriseplan oppdatert i løpet av de to siste årene	:	14	27
IT-sikkerhetsveiledning for alle brukere, oppdatert i løpet av de to siste årene	:	12	25
Filtrering av innkommende e-post (spam-beskyttelse)	:	44	70
Oppdatert noen sikkerhetstiltak, f.eks. antivirusprogram, i løpet av de seneste tre månedene	70	81	82

Kilde: Statistisk sentralbyrå.

7.3. IKT-sikkerhet i offentlig sektor

Dette avsnittet beskriver omfanget av noen problemer knyttet til IKT-bruk og hvilke sikkerhetstiltak som var gjennomført i offentlig sektor i 2005.

- Antivirusprogam, brannmurer og spam-filtre benyttes av nesten samtlige offentlige enheter. På tross av dette var det relativt utbredt med virusangrep, ormer eller lignende som resulterte i tap av data eller arbeidstid.
- De fleste offentlige enheter har formalisert ansvaret for IT-sikkerheten ved å utnevne en ansvarlig person. Om lag halvparten av enhetene gjennomfører løpende IT-sikkerhetsutdanning av medarbeidere.

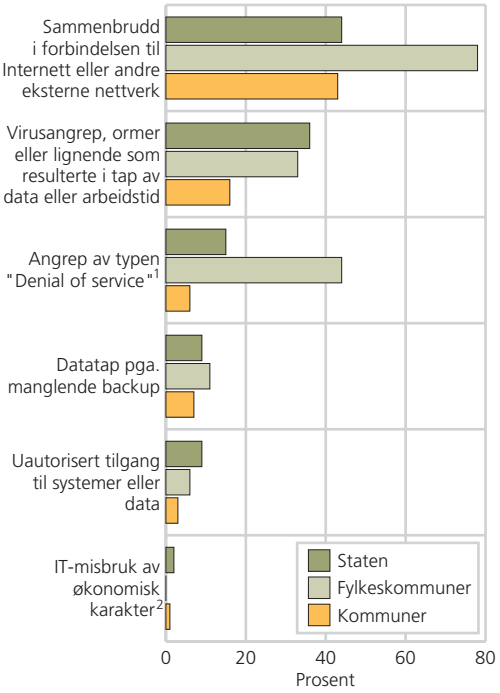
Problemer knyttet til bruk av IKT

- Virusangrep, ormer eller lignende som førte til tap av data og/eller arbeidstid hadde oppstått blant 36, 33 og 16 prosent av henholdsvis statlige foretak, fylkeskommuner og kommuner i 2005.
- Tilsvarende hadde tap av data på grunn av manglende backup oppstått blant 11, 9 og 7 prosent av fylkeskommunene, statlige foretak og kommunene.
- IT-misbruk av økonomisk karakter som for eksempel bedrageri eller manipulasjon av data var lite utbredt i 2005.

Organisatoriske forhold

- I 2005 hadde 88 prosent av fylkeskommunene utnevnt en ansvarlig person for IT-sikkerheten. Blant statlige foretak og i kommunene hadde henholdsvis 81 og 71 prosent gjort det samme. Løpende IT-sikkerhetsutdanning av medarbeidere ble gjennomført blant 53 prosent av fylkeskommunene, 47 prosent av statlige foretak og 41 prosent blant kommunene.
- En beredskapsplan som er ajourført i løpet av de to siste årene var minst vanlig blant fylkeskommunene med 18 prosent. Dette representerer en nedgang på 15 prosentpoeng fra året før. Blant statlige foretak og kommunene var det 44 og 37 prosent som hadde en oppdatert beredskapsplan i 2005.

Figur 7.3.1. Andel kommuner, fylkeskommuner og statlige foretak som har vært utsatt for følgende problemer. 2005. Prosent



[1] Handling(er) som forhindrer deler av et system eller nettverk å fungere ordentlig, for eksempel store mengder forespørsler.
[2] For eksempel bedrageri, manipulasjon av data.
Kilde: Statistisk sentralbyrå.

Sikkerhetstiltak

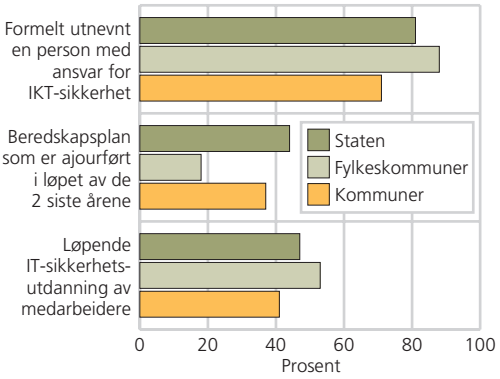
- Tilnærmet alle enheter i offentlig sektor har brannmur og løpende abonnement på antivirusprogram. Spam-filtre benyttes av rundt 90 prosent av de samme enhetene.
- Program som avdekker og varsler uventet/uønsket trafikk (Intrusion detection) var minst utbredt og ble benyttet av rundt 60 prosent av alle enheter i offentlig sektor.

Om statistikken

Datagrunnlaget for offentlig sektor er hentet fra Statistisk sentralbyrås undersøkelser om bruk av IKT i henholdsvis kommunene, fylkeskommunene og staten. Alle undersøkelsene er fulltellinger og staten er definert som alle foretak innenfor stats- og trygdeforvaltningen, statens forretningsdrift, statlige låneinstitusjoner, statsforetak (100 prosent eid av staten) samt Norges Bank. Oslo inngår i kommunetallene og ikke i fylkestallene. Ytterligere detaljer om undersøkelsene er beskrevet i kapittel 6.

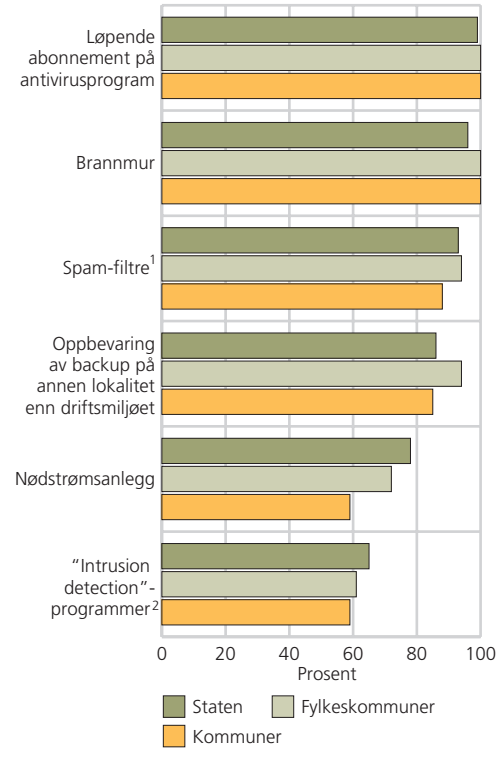
Internett-referanser: www.ssb.no/iktbrukk/
www.ssb.no/iktbruks/

Figur 7.3.2. Andel kommuner, fylkeskommuner og statlige foretak med ulike sikkerhetstiltak. 2005. Prosent



Kilde: Statistisk sentralbyrå.

Figur 7.3.3. Andel kommuner, fylkeskommuner og statlige foretak med ulike sikkerhetssystemer. 2005. Prosent



[1] Filtrering av innkommende e-post.
[2] Program for avdekking og varsling av uønsket/uventet trafikk.
Kilde: Statistisk sentralbyrå.

Tabell 7.3.1. Andel kommuner, fylkeskommuner og statlige foretak som har vært utsatt for følgende problemer. 2005. Prosent

	IT-misbruk av økonomisk karakter[1]	Uautorisert tilgang til systemer eller data	Angrep av typen "Denial of service"[2]	Datatap pga. manglende backup	Virusangrep, ormer eller lignende som resulterte i tap av data eller arbeidstid	Sammenbrudd i forbindelsen til Internett
Andel kommuner	1	3	6	7	16	43
Andel fylkeskommuner	0	6	44	11	33	78
Andel statlige foretak	2	9	15	9	36	44

[1] For eksempel bedrageri, manipulasjon av data.
[2] Handling(er) som forhindrer deler av et system eller nettverk å fungere ordentlig, for eksempel store mengder forespørsler.
Kilde: Statistisk sentralbyrå.

Tabell 7.3.2. Andel kommuner, fylkeskommuner og statlige foretak med ulike sikkerhetstiltak. 2004 og 2005. Prosent

	Formelt utnevnt en person med ansvar for IKT-sikkerhet	Beredskapsplan som er ajourført i løpet av de to siste årene	Løpende IT-sikkerhetsutdanning av medarbeidere
2004			
Andel kommuner	73	30	23
Andel fylkeskommuner	83	33	44
Andel statlige foretak	77	40	36
2005			
Andel kommuner	71	37	41
Andel fylkeskommuner	88	18	53
Andel statlige foretak	81	44	47

Kilde: Statistisk sentralbyrå.

Tabell 7.3.3. Andel kommuner, fylkeskommuner og statlige foretak med ulike sikkerhetssystemer. 2005. Prosent

	Nødstrømsanlegg	Oppbevaring av backup på annen lokalitet enn driftsmiljøet	Brannmur	Løpende abonnement på antivirusprogram	Spamfiltre[1]	"Intrusion detection"-programmer[2]
Andel kommuner	59	85	100	100	88	59
Andel fylkeskommuner .	72	94	100	100	94	61
Andel statlige foretak ...	78	86	96	99	93	65

[1] Filtrering av innkommende e-post.
[2] Program for avdekking og varsling av uønsket/uventet trafikk.
Kilde: Statistisk sentralbyrå.

7.4. IKT-sikkerhetsproblemer og -tiltak blant privatpersoner

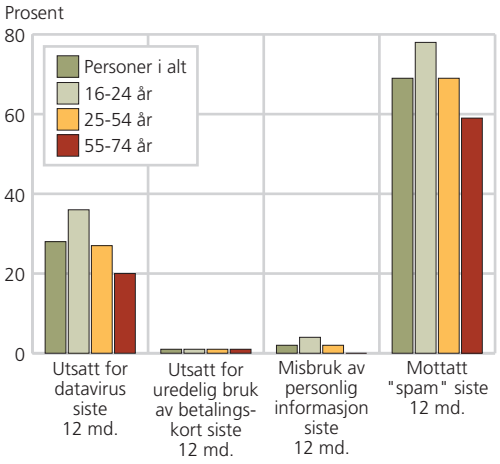
Avsnittet tar for seg IKT-sikkerhetsproblemer, og -tiltak mot disse. Tallene er fra 2. kvartal 2005. Med Internett-bruker menes det her en som har brukt Internett de siste tolv månedene.

- Knapt tre av ti av Internett-brukere har blitt utsatt for datavirus.
- Så godt som alle har oppdatert antivirusprogram eller brannmur på datamaskinen hjemme.

Mindre datavirus

- Det er en nedgang i antall personer som har blitt utsatt for datavirus fra 33 prosent i 2004 til 28 prosent i 2005. Det er de yngste Internett-brukerne som oftest blir utsatt for datavirus.
- Sju av ti Internett-brukere har mottatt "spam" de siste tolv månedene. De yngre Internett-brukerne mottar oftere "spam" enn de eldre.
- Når det gjelder mer alvorlige sikkerhetsproblemer, slik som å bli utsatt for uredelig bruk av betalingskort eller misbruk av personlig informasjon, er dette noe henholdsvis 1 og 2 prosent av Internett-brukerne blir utsatt for.

Figur 7.4.1. Sikkerhetsproblemer etter alder. Andel av de som har vært på Internett siste 12 md. 2005. Prosent

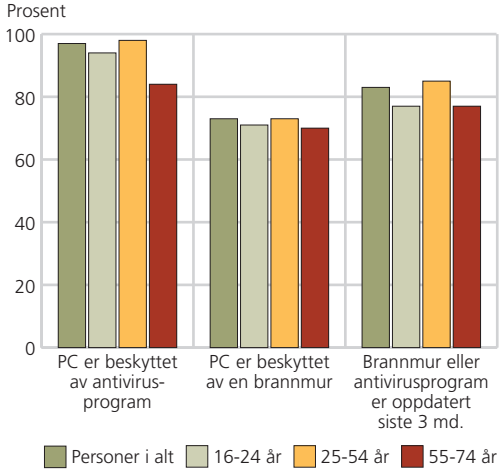


Kilde: Statistisk sentralbyrå.

Antivirusprogram på nesten alle datamaskiner

- Det er utbredt med sikkerhetstiltak på datamaskinene hjemme. 83 prosent har oppdatert antivirusprogram eller installert brannmur i løpet av de siste tre måneder på datamaskinen hjemme.
- Ifølge vår undersøkelse har 97 prosent antivirusprogram på datamaskinen hjemme. Sett i en nordisk sammenheng er dette tallet høyt. Tilsvarende tall for Danmark og Sverige er henholdsvis 93 og 88 prosent. Siden tallene er basert på utvalg, må vi ta i betraktning at det kan være usikkerheter knyttet til tallene, og at det reelle tallet derfor kan være noe lavere.
- Det er kun små forskjeller mellom alder og kjønn når det gjelder utbredelsen av sikkerhetstiltakene.

Figur 7.4.2. Sikkerhetstiltak på datamaskinen hjemme, etter alder. Andel av de som har vært på Internett siste 3 md. hjemme. 2005. Prosent



Kilde: Statistisk sentralbyrå.

Om statistikken

Datagrunnlaget er hentet fra Statistisk sentralbyrås undersøkelse om bruk av IKT i husholdningene. Statistikken omfatter et utvalg av den norske befolkningen fra og med 16 år til og med 74 år og deres bruk av og tilgang til IKT. Den enkelte person er statistisk enhet. For spørsmål som gjelder husholdningen, for eksempel typer IKT som respondenten har hjemme, er også husholdningen statistisk enhet. Til husholdningen regnes alle personer som er fast bosatt i boligen, og som har felles matbudsjett. Utvalget inneholder 2 000 personer og svarprosenten ligger på vel 60. Dataene blir innhentet i 2. kvartal i referanseåret.

Internett-referanse: www.ssb.no/ikthus/

Tabell 7.4.1. Andel av de som har brukt Internett siste 12 md. som har vært utsatt for sikkerhetsproblemer, etter kjønn, alder, utdanning og arbeidssituasjon. 2005. Prosent

	Utsatt for datavirus siste 12 md.		Utsatt for uredelig bruk av bet.-kort siste 12 md.		Misbruk av personlig informasjon siste 12 md.		Mottatt "spam" siste 12 md.	
	2004	2005	2004	2005	2004	2005	2004	2005
Personer i alt	**33**	**28**	**2**	**1**	**3**	**2**	**71**	**69**
Kjønn								
Menn	35	32	2	1	3	2	73	72
Kvinner	30	24	1	1	2	2	69	67
Alder								
16-24 år	32	36	1	1	3	4	80	78
25-54 år	35	27	3	1	3	2	71	69
55-74 år	24	20	0	1	1	0	60	59
Utdanning								
Ungdomsskole	23	26	3	0	5	4	66	69
Videregående skole	31	30	1	1	2	2	70	69
Universitet/høyskole +	38	24	2	1	3	2	73	71
Arbeidssituasjon								
Ansatt eller selvstendig næringsdrivende	33	28	2	1	2	1	70	69
Student	33	34	1	1	2	5	86	80
Pensjonist	35	20	1	1	1	1	59	51
Arbeidsledig eller annet (inkl. førstegangstj., hjemmeværende)	29	16	2	1	6	0	63	49

Kilde: Statistisk sentralbyrå.

7.5. Regionale perspektiv

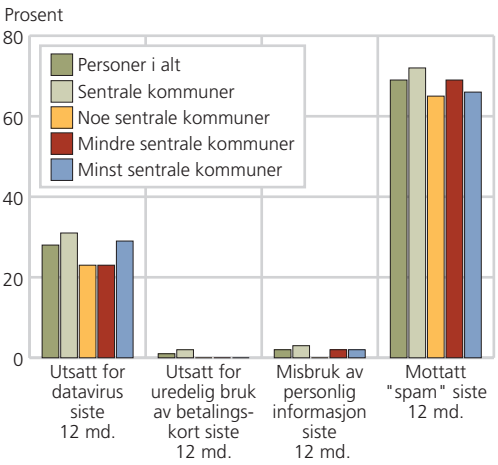
For å belyse regionale forskjeller vedrørende IKT-sikkerhet i husholdningene, har vi tatt utgangspunkt i Statistisk sentralbyrås Standard for kommuneklassifisering. Personene som har besvart undersøkelsen IKT i husholdningene er fordelt etter hvilken kommune de bor i. Det er fire sentralitetskoder for kommunene: sentrale kommuner, noe sentrale kommuner, mindre sentrale kommuner og minst sentrale kommuner. Avsnittet inneholder også tall for fylkesvis fordeling av virusangrep i næringslivet og bruk av viruskontroll og beskyttelsesprogramvare.

- Det er meget små forskjeller i IKT-sikkerhetsproblemer og -tiltak mellom personer i sentrale og øvrige kommuner.
- Virusangrep rammet næringslivet i alle fylker like hardt, og over alt brukte foretakene viruskontroll.

Ingen regionale forskjeller mellom personer

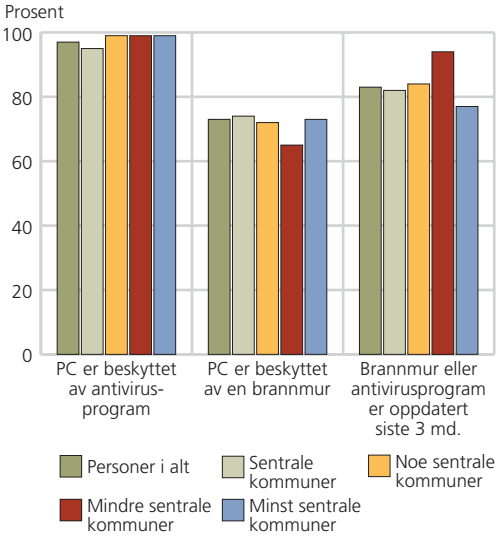
- En kan se en svak tendens til at sentrale kommuner er mer utsatt for sikkerhetsproblemer. For de noe sentrale, mindre sentrale og minst sentrale kommunene ser sikkerhetsproblemene ut til å være på et likt nivå.
- Det er kun små forskjeller mellom sentrale og øvrige kommuner når det gjelder sikkerhetstiltak på PC-en hjemme.

Figur 7.5.1. Andel av de som har vært på Internett de siste 12 md. som har vært utsatt for sikkerhetsproblemer, fordelt etter sentralitet. 2005. Prosent



Kilde: Statistisk sentralbyrå.

Figur 7.5.2. Sikkerhetstiltak fordelt etter sentralitet. Andel av de som har vært på Internett hjemme de siste 3 md. 2005. Prosent

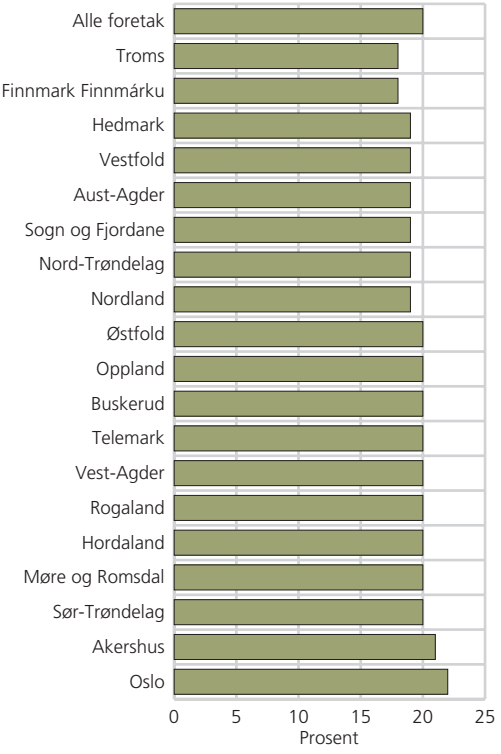


Kilde: Statistisk sentralbyrå.

Heller ingen regionale forskjeller mellom foretak

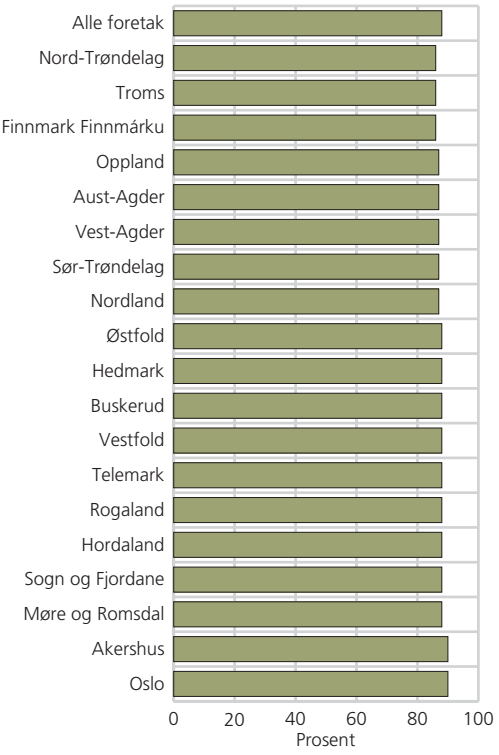
- Tallene viser ingen regionale forskjeller for andel foretak rammet av virusangrep. Om lag 20 prosent av foretakene ble rammet av virusangrep i alle fylkene. Forskjellen mellom fylkene er ikke større enn 4 prosentpoeng.
- Det er små forskjeller mellom fylkene i bruk av viruskontroll og beskyttelsesprogramvare. Over alt bruker knapt 90 prosent av foretakene dette sikkerhetstiltaket.

Figur 7.5.3. Andel av alle foretak rammet av virusangrep, fordelt etter fylke. Foretak med 10+ sysselsatte. 2005. Prosent



Kilde: Statistisk sentralbyrå.

Figur 7.5.4. Andel av foretak som brukte viruskontroll og beskyttelsesprogramvare, fordelt etter fylke. Foretak med 10+ sysselsatte. 2005. Prosent



Kilde: Statistisk sentralbyrå.

Om statistikken

Datagrunnlaget for personer er hentet fra samme statistikk som beskrevet i avsnitt 7.4, mens dataene for næringslivet blir beskrevet i avsnitt 7.2.

Internett-referanser: www.ssb.no/ikthus/
www.ssb.no/iktbrukn/

7.6. Internasjonale perspektiv

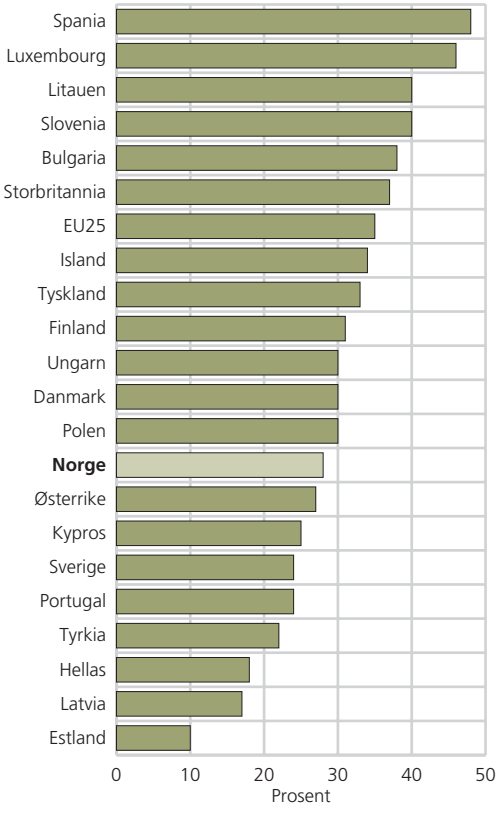
Avsnittet sammenligner sikkerhetsproblem og -tiltak i norske husholdninger og foretak med forholdene i mange europeiske land. Avsnittet omfatter også sammenligninger mellom danske og norske kommuner når det gjelder bruk av digitale signaturer, samt sikkerhetsproblemer og -tiltak.

- Norske husholdninger er mindre utsatt for datavirus enn gjennomsnittet i EU og ligger i tetsjiktet i europeisk sammenheng når det gjelder sikkerhetstiltak.
- Norske foretak blir utsatt for virusangrep noe sjeldnere enn i EU og oppdaterer sikkerhetstiltak hyppigere enn gjennomsnittet i EU-landene.
- Danske kommuner ligger langt foran norske kommuner når det gjelder bruk av digitale signaturer. Til gjengjeld er danske kommuner mer utsatt for ulike problemer knyttet til IT-sikkerhet. Det er små forskjeller mellom Danmark og Norge når det gjelder ulike organisatoriske sikkerhetstiltak som er gjennomført i kommunene.

Nordmenn mindre utsatt for datavirus enn EU-gjennomsnittet

- Norge ligger 7 prosentpoeng under EU-gjennomsnittet når det gjelder å bli utsatt for datavirus i hjemmet. Sverige ligger 4 prosentpoeng under Norge, mens Danmark ligger 7 prosentpoeng over Norge. Spania er landet som i størst grad blir utsatt for datavirus.
- Når det gjelder å bli utsatt for misbruk av personlig informasjon over Internett, ligger Norge 1,9 prosentpoeng under EU-gjennomsnittet.

Figur 7.6.1. Andel personer av de som har brukt Internett de siste 12 md. og som har vært utsatt for datavirus. 2005. Prosent

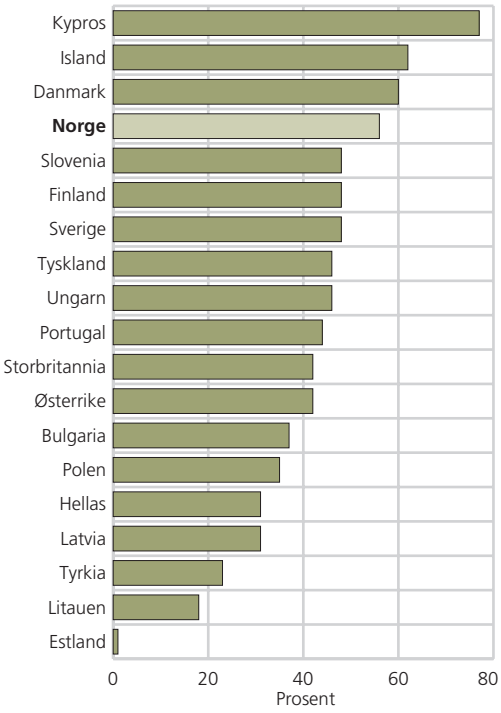


Kilde: Eurostat.

Nordmenn oppdaterer antivirusprogram oftere enn de fleste

- Ifølge tall fra 2004 ligger Norge på en fjerdeplass i europeisk sammenheng når det gjelder å oppdatere antivirusprogram på PC. Det finnes i skrivende stund ikke internasjonale data for 2005 for sikkerhetstiltak. Det er med andre ord 56 prosent av de som har brukt Internett siste tre måneder (altså 1. kvartal 2004) som har oppdatert antivirusprogram. De landene som har en høyere andel er Kypros, Island og Danmark med henholdsvis 77, 62 og 60 prosent. Det er de baltiske landene som i minst grad har oppdaterte antivirusprogram.

Figur 7.6.2. Andel personer av de som har brukt Internett de siste 3 md. som har oppdatert antivirusprogram de siste 3 md. 2004. Prosent

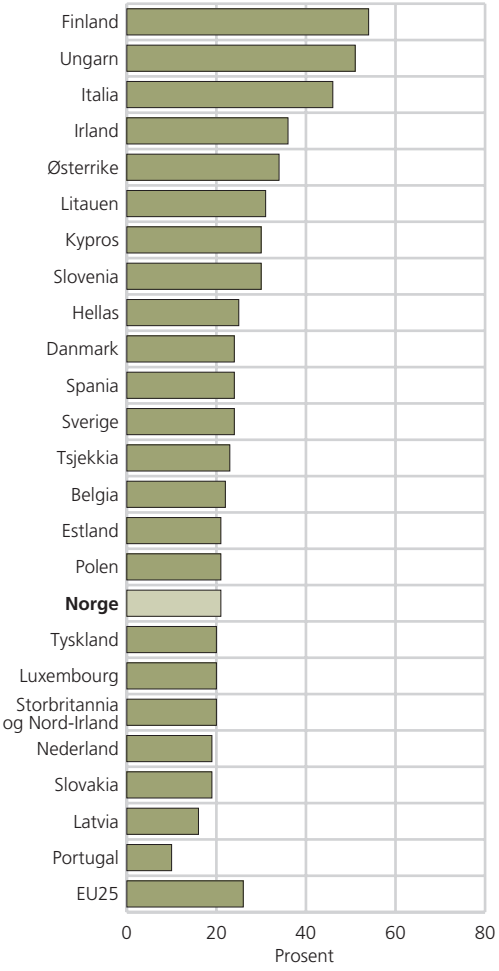


Kilde: Eurostat.

Hyppig oppdatering av antivirusprogram i norske foretak

- Andelen av alle foretak utsatt for virusangrep siste året er noe lavere i Norge enn i EU med henholdsvis 21 og 26 prosent. Foretak i Sverige og Danmark ligger på samme nivå som norske med 24 prosent, mens finske foretak er langt mer utsatt for virusangrep. Andelen foretak utsatt for virusangrep siste året er på hele 54 prosent i Finland.

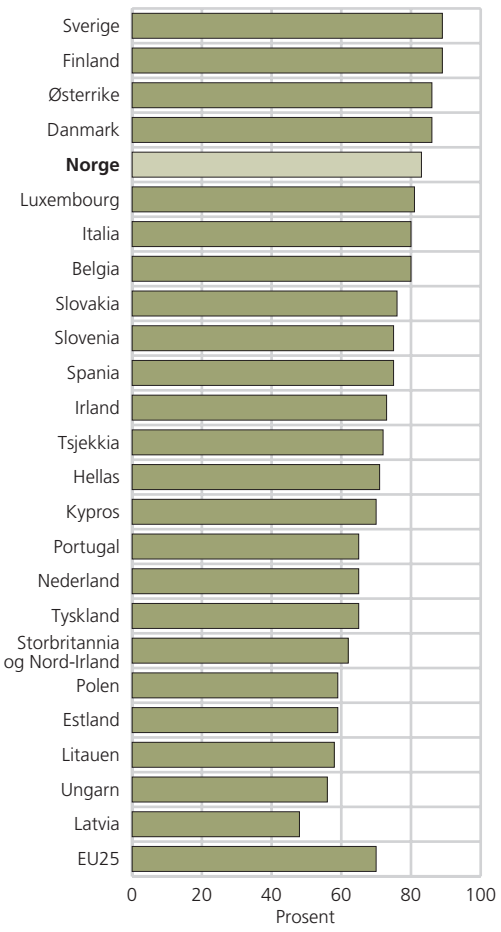
Figur 7.6.3. Andel av alle foretak utsatt for virusangrep siste året. Foretak med 10+ sysselsatte. 2005. Prosent



Kilde: Eurostat.

- Andelen av alle norske foretak som har oppdatert noen sikkerhetstiltak (for eksempel antivirusprogrammer) de siste tre månedene er klart høyere enn gjennomsnittet i EU, henholdsvis 83 og 70 prosent. Bare næringslivet i Finland, Sverige, Østerrike og Danmark oppdaterer sikkerhetstiltak hyppigere. I Latvia har under halvparten av foretakene gjennomført en oppdatering i løpet av de siste tre månedene. Forskjellig utbredelse av Internett-tilgang påvirker omfanget av sikkerhetsproblemer og hyppigheten av oppdateringen av sikkerhetstiltak.

Figur 7.6.4. Andel av alle foretak som har oppdatert noen sikkerhetstiltak de siste 3 md. Foretak med 10+ sysselsatte. 2005. Prosent

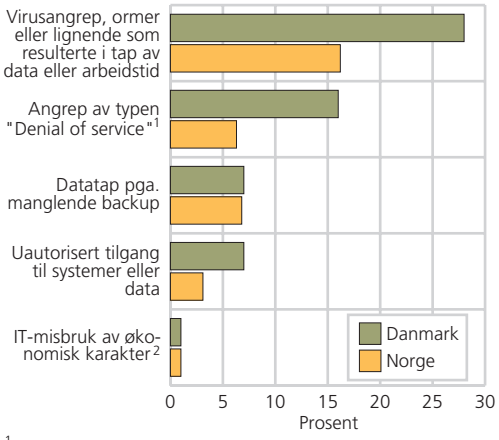


Kilde: Eurostat.

Norske kommuner mindre utsatt for sikkerhetsproblemer enn danske

- I Danmark hadde 28 prosent av kommunene vært utsatt for virusangrep, ormer eller lignende som hadde resultert i tap av data eller arbeidstid, mot 16 prosent av kommunene i Norge. Angrep av typen "Denial of service" og uautorisert adgang til systemer eller data var også et større problem i Danmark enn i Norge. Tap av data på grunn av manglende backup hadde vært et problem hos 7 prosent av kommunene i både Danmark og Norge.

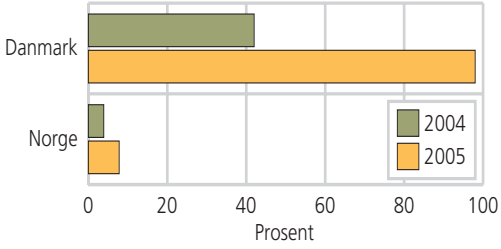
Figur 7.6.5. Andel kommuner i Danmark og Norge som har vært utsatt for problemer i forhold til IT-sikkerhet. 2005. Prosent



[1] Handling(er) som forhindrer deler av et system eller nettverk å fungere ordentlig, for eksempel store mengder forespørsler.
[2] For eksempel bedrageri, manipulasjon av data.
Kilde: Danmarks Statistik og Statistisk sentralbyrå.

- I 2005 benyttet 98 prosent av de danske kommunene digitale signaturer for å identifisere brukere av elektroniske tjenester. Tilsvarende andel i 2004 var 42 prosent. Her ligger Norge langt etter Danmark. I 2005 benyttet 8 prosent av de norske kommunene digitale signaturer for å identifisere sine brukere av elektroniske tjenester.

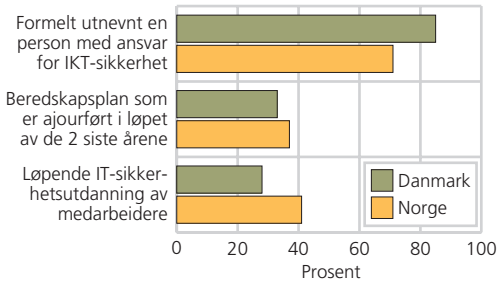
Figur 7.6.6. Andel kommuner i Danmark og Norge som benytter digital signatur for å identifisere brukere. 2004 og 2005. Prosent



Kilde: Danmarks Statistik og Statistisk sentralbyrå.

- Formell utnevnelse av en person med ansvar for IT-sikkerheten var mer vanlig i Danmark enn i Norge i 2005. Løpende IT-sikkerhetsutdanning av medarbeidere var til gjengjeld mer vanlig i Norge enn i Danmark. Det samme gjelder beredskapsplaner som var oppdatert i løpet av de to siste årene.

Figur 7.6.7. Andel kommuner i Danmark og Norge med ulike sikkerhetstiltak. 2005. Prosent



Kilde: Danmarks Statistik og Statistisk sentralbyrå.

Om statistikken

Datagrunnlaget for personer og husholdninger er hentet fra samme statistikk som beskrevet i avsnitt 7.4, mens dataene for næringslivet blir beskrevet i avsnitt 7.2. De internasjonale tallene er hentet fra EUs statistiske kontor Eurostat.

Datagrunnlaget for offentlig sektor er hentet fra den samme statistikken som er beskrevet i avsnitt 6.1, mens de danske tallene er hentet fra tilsvarende undersøkelse i Danmark. I dette kapitlet er det kun tatt med et utvalg variabler som er sammenlignbare mellom de to landene.

Internett-referanser: http://www.ssb.no/iktk
http://www.dst.dk/Statistik/IT/Myndigheder.aspx
http://epp.eurostat.cec.eu.int

Tabell 7.6.1. Andel av alle foretak utsatt for virusangrep siste året. Foretak med 10+ sysselsatte, etter land. 2003-2005. Prosent

	2003	2004	2005
EU25	:	26	26
Belgia	34	29	22
Tsjekkia	:	27	23
Danmark	45	32	24
Tyskland	:	23	20
Estland	:	36	21
Hellas	43	27	25
Spania	:	29	24
Irland	:	41	36
Italia	44	22	46
Kypros	:	28	30
Latvia	:	17	16
Litauen	:	33	31
Luxembourg	24	32	20
Ungarn	:	22	51
Malta	26	:	:
Nederland	29	41	19
Østerrike	29	32	34
Polen	:	22	21
Portugal	20	26	10
Slovenia	:	29	30
Slovakia	:	16	19
Finland	40	51	54
Sverige	30	30	24
Storbritannia og Nord-Irland	:	:	20
Bulgaria	:	15	:
Romania	:	15	:
Island	26	:	:
Norge	36	25	21
Japan	74	:	:
Korea	:	44	:
Australia	53	:	:

Kilde: Eurostat.

Tabell 7.6.2. Andel av alle foretak som har oppdatert sikkerhetstiltak seneste 3 md. Foretak med 10+ sysselsatte, etter land. 2003-2005. Prosent

	2003	2004	2005
EU25	:	73	70
Belgia	79	88	80
Tsjekkia	:	67	72
Danmark	80	88	86
Tyskland	72	81	65
Estland	:	51	59
Hellas	63	61	71
Spania	28	74	75
Irland	:	72	73
Italia	52	73	80
Kypros	:	66	70
Latvia	:	53	48
Litauen	:	45	58
Luxembourg	66	:	81
Ungarn	:	48	56
Malta	59	:	:
Nederland	74	76	65
Østerrike	78	87	86
Polen	:	49	59
Portugal	48	61	65
Slovenia	:	66	75
Slovakia	:	60	76
Finland	84	89	89
Sverige	79	89	89
Storbritannia og Nord-Irland	:	:	62
Bulgaria	:	47	:
Romania	:	23	:
Island	79	:	:
Norge	68	76	83

Kilde: Eurostat.