

# DATASIKKERHEDEN I DANMARK ÅR 2000

## **Forord**

Med denne publikation søger IT-Sikkerhedsrådet at opfylde det led i sit kommissorium, der pålægger Rådet at afgive en årlig vurdering af datasikkerheden i Danmark. I sin årsberetning for 1999 konstaterede Rådet, at det var vanskeligt at afgive en sådan kvalificeret status uden statistiske oplysninger om samfundets IT-relaterede sårbarhed. Sådanne forelå hverken fra officielt hold eller hos forsikringsbranchen.

Under sit møde den 28. august 2000- og under medvirken af Rådets panel af eksterne sagkyndige - besluttede Rådet derfor at gennemføre en uvildig undersøgelse af området, samt løbende at følge udviklingen i de skader, der rammer IT-behandlingen og dermed virker som hæmsko for udviklingen af en velfungerende IT-infrastruktur.

"Datasikkerheden i Danmark år 2000" udgør en delrapport af denne undersøgelse, der gennemføres over en 3-årig periode. Denne første fase omfatter perioden 1. januar 2000 til 31. december 2000.

Undersøgelsen er i international sammenhæng enestående ved både at være flerårig, landsdækkende, uvildig og gennemført 100% anonymt. De medvirkende virksomheder er sikret anonymitet. Kun IT- og Forskningsministeriet råder over adresser og kontaktpersoner på de deltagende virksomheder, men ikke deres besvarelser. Derimod har kun det medvirkende analyseinstitut – PricewaterhouseCoopers - adgang til selve besvarelserne, men ikke til hvilke virksomheder der deltager. Denne anonymitet sikrer, at virksomhederne kan besvare intrikate spørgsmål om beskyttelsesforanstaltninger og indtrufne skader uden at skulle stå frem selv og uden risiko for eksponering, selv om deres besvarelse skulle falde i uvedkommendes hænder.

Det er IT-Sikkerhedsrådets håb, at de indhentede resultater vil give et godt fundament for at følge udviklingen på området, såvel på sikringsniveauet som på skadesbilledet. Det er ligeledes Rådets håb, at resultatet kan bidrage væsentligt til en bedre datasikkerhed i Danmark.

Som nævnt er undersøgelsen gennemført ved PricewaterhouseCoopers som analyseinstitut under projektledelse af medlem af IT-Sikkerhedsrådet, direktør Jan Carlsen. I analysearbejdet hos PricewaterhouseCoopers har endvidere Manager Pernille Plambech og Analytiker Mona Ayub Syed deltaget. I IT- og Forskningsministeriet har chefkonsulent Palle H. Sørensen og kontorfuldmægtig Anni Grønlund medvirket.

IT-Sikkerhedsrådet retter en stor tak til de medvirkende ca. 450 virksomheder, der velvilligt har stillet deres viden og ressourcer til rådighed for undersøgelsen. Forhåbentlig viser en gennemlæsning af denne rapport hvilken værdi denne synliggørelse af IT-sikkerheden i Danmark kan have for den sikkerhedspolitiske diskussion.

Mads Bryde Andersen  
Professor, dr.jur.  
Formand for IT-Sikkerhedsrådet

## **Indholdsfortegnelse**

1 Kort om undersøgelsen	4
2 Stamrapporteringerne	5
2.1 Spørgeskema	5
2.2 Vurdering af svar - "Best Quality"	6
2.3 Sikkerhedsniveauet i forskellige virksomhedstyper m.v.	7
2.4 IT-sikkerheden i forhold til virksomhedens størrelse	8
2.5 IT-sikkerheden i industrien	9
2.6 Rådets kommentarer til stamrapporteringerne	9
3 Hændelsesrapporteringerne år 2000	12
3.1 Undersøgelsen	12
3.2 Hit-listen for uheld, skader m.v.	13
3.3 Hit-listen efter skadernes konsekvenser	14
3.4 Fordelingen af skader i den offentlige og den private sektor	14
3.5 Fordeling af skader på virksomhedernes størrelse	15
3.6 Hit-listens skader fordelt på virksomheds størrelser m.v.	15
3.7 Hit-listens skader fordelt på brancher	16
3.8 Rådets kommentarer til hændelsesrapporteringerne	16
4 Det videre arbejde	19
Bilag 1 Detaljer vedrørende de indtrufne hændelser	20
Bilag 2 Omkring undersøgelsen	45
Bilag 3 Stamregistreringsskema	49
Bilag 4 Hændesskema	55

## **1. Kort om undersøgelsen**

Som nævnt i forordet indeholder denne redegørelse resultaterne fra den første fase i IT-Sikkerhedsrådets kortlægning af datasikkerheden i Danmark, omfattende perioden 1. januar 2000 til 31. december 2000.

Til brug for undersøgelsen har Danmarks Statistik udvalgt 1.200 virksomheder indenfor den offentlige og private sektor, som et repræsentativt udsnit af danske virksomheder og institutioner. Samtidig har IT- og Forskningsministeriet og IT-Sikkerhedsrådets medlemmer peget på ca. 400 virksomheder og institutioner som formodede "tungere" IT-anvendere til yderligere at indgå i undersøgelsen.

I alt ca. 1.600 virksomheder og institutioner har derefter modtaget en invitation om at deltage. Af disse meldte ca. 458 sig, hvoraf 441 har indsendt besvarelser. Dette er en svarprocent på ca. 27,6, hvilket må anses for et tilfredsstillende resultat for en 3-årig undersøgelse.

Besvarelserne er foretaget på 2 skemaer.

Det første skema "Staminformationer" udsendtes i november 2000 og omfatter virksomhedernes aktuelle beskyttelsesforanstaltninger.

Det andet skema "Hændelsesregistreringer" udsendtes medio januar 2001 og indeholder rapporteringer om de hændelser eller skader som de deltagende virksomheder har været udsat for i løbet af år 2000.

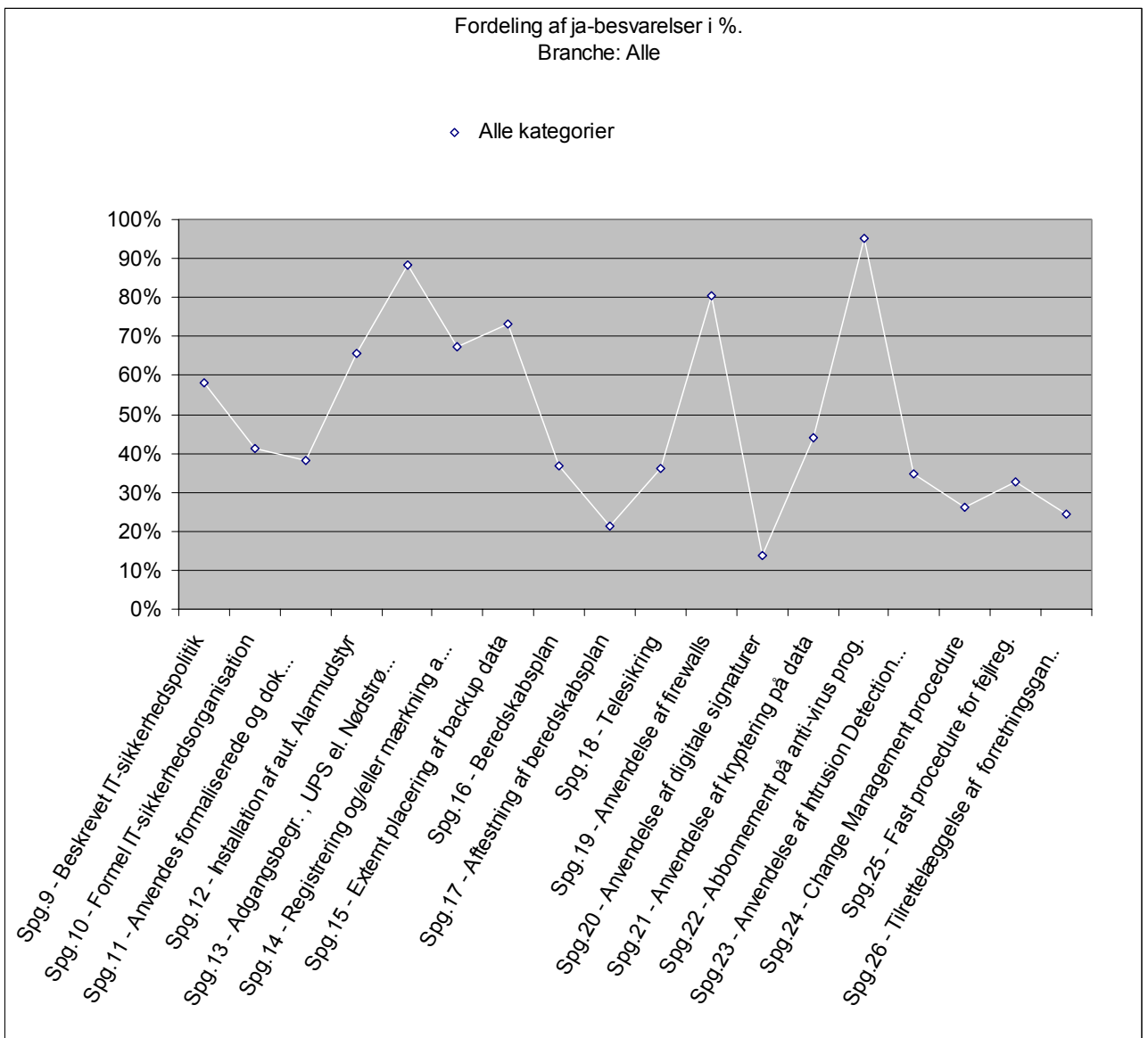
For nærmere specifikationer af spørgeskemaer og grupperinger af besvarelser, se bilag 2 til undersøgelsen.

## 2. Stamrapporteringerne

### 2.1 Spørgeskemaet

Stamregistreringerne er fortaget på skema, som vist i bilag 3, der indeholder i alt 26 hovedspørgsmål. De første 8 handler om virksomheden og dens anvendelse af IT. De resterende 18 vedrører forskellige sikringsforanstaltninger, som deltagerne svarer "Ja" eller "Nej" til. Svaret "Ja", er der for de fleste spørgsmål yderligere mulighed for at angive dybden eller kvalitetsniveauet af de indførte foranstaltninger.

Vist på en graf efter de stillede spørgsmål, ser besvarelserne således ud:



## 2.2 Vurdering af svar – "Best Quality"

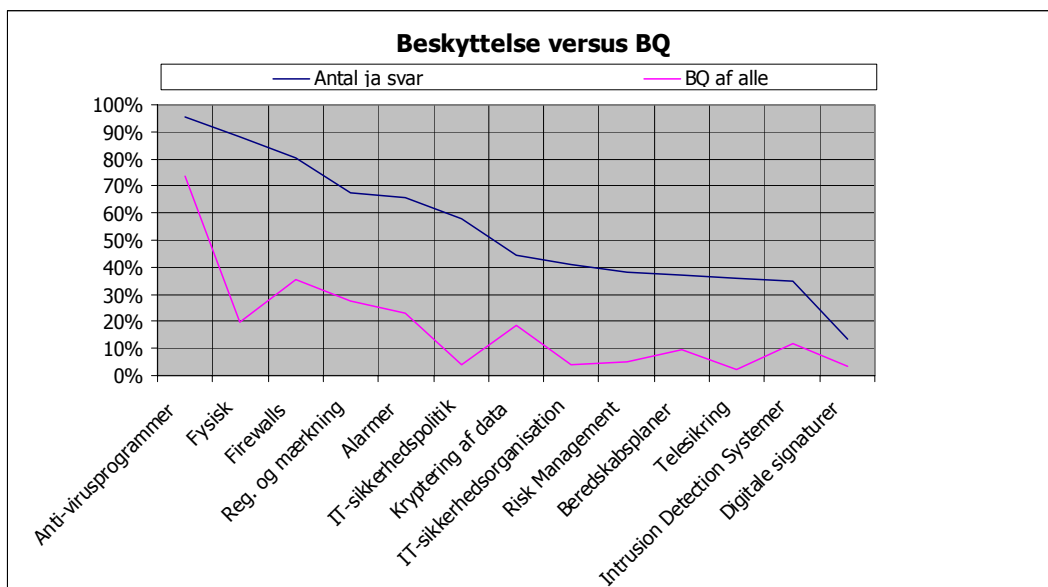
Når man vælger en spørgeteknik som den anvendte, løber man risikoen for at få uensartede svar. Selv om en respondent måtte svare "Ja" på et spørgsmål om, hvorvidt en given sikringsforanstaltning er indført, kan der være stor forskel på kvaliteten af den pågældende foranstaltning. Hvad en virksomhed må anses for at udgøre en "IT-sikkerhedspolitik", falder måske helt uden for den betydning, en anden virksomhed måtte have om dette begreb.

For at tage højde for denne usikkerhed er hvert af de stillede spørgsmål om sikringsforanstaltninger - hvor dette er muligt<sup>1</sup> - tildelt en værdi for "Best Quality" (BQ) baseret på besvarelse af et eller flere af underliggende spørgsmål. BQ-værdien udgør altså den del af JA-besvarelserne, som kendetegnes ved, at der også er svaret ja til et eller flere underliggende spørgsmål, der siger noget om værdien af hovedspørgsmålet. Ud fra de angivne underspecifikationer kan man altså konstatere, hvad der *ud fra de stillede spørgsmål* repræsenterer den bedste sikkerhed.

Et eksempel vil illustrere dette:

Når 44,1% af deltagerne f.eks. har svaret "Ja" til spørgsmålet, om de anvender kryptering på hele eller dele af deres kommunikation, stilles der to efterfølgende spørgsmål. I det ene spørges der, om kryptering anvendes frivilligt og kun i det omfang det er standard i systemet. Det andet spørger, om det er obligatorisk at kryptere al kritisk kommunikation. Da den bedste sikkerhed utvivlsomt opnås, såfremt det andet spørgsmål er afkrydset, anses en sådan afkrydsning for at repræsentere "BQ". I dette tilfælde er BQ følgelig kryds i Ja for anvendelse af kryptering og kryds under det andet underspørgsmål. Det har lidt under halvdelen (42,1%) af de, der havde besvaret hovedspørgsmålet med "Ja", svarende til 18,6% af samtlige deltagere.

Overføres disse principper til nedenstående graf kan den tolkes som følger:



Området over den sorte (øverste) kurve viser det procentvise antal virksomheder, der ikke har sikringstiltag på de anførte områder.

<sup>1</sup> Følgende spørgsmål har ingen underspecifikationer: Placering af backup, Change Management, procedure for registrering af fejl og forsinkelser samt parathed til efterlevelen af Persondataloven.

Området under den sorte streg viser de virksomheder, der har besvaret spørgsmålet om sikringsforanstaltninger på området med et JA og følgelig har sådanne foranstaltninger i et eller andet omfang.

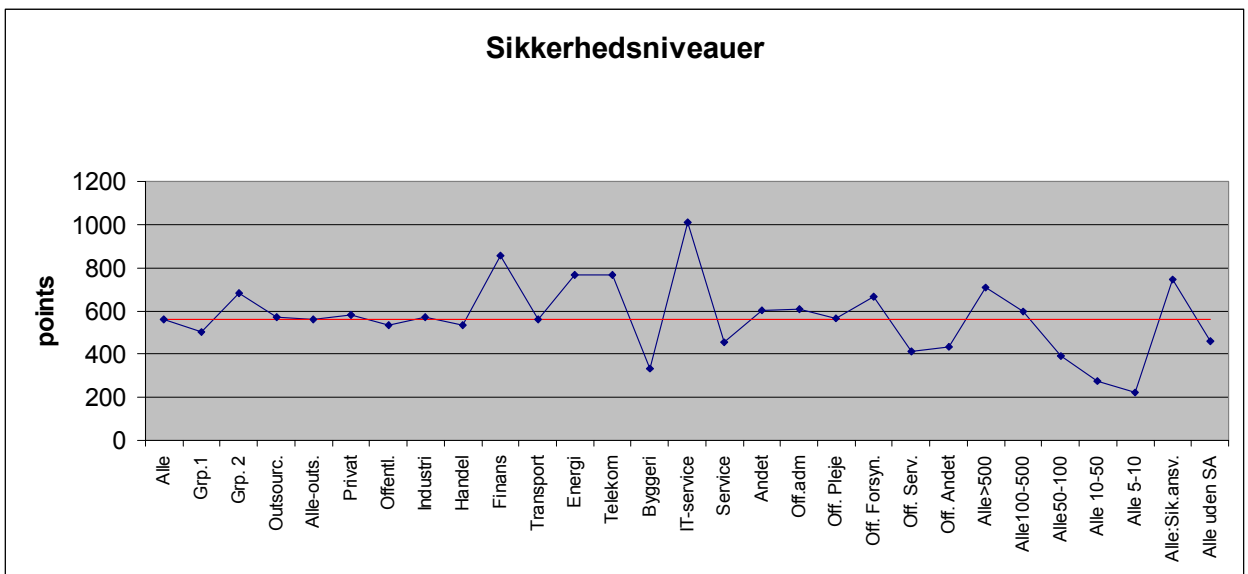
Området under den røde (underste) kurve viser det procentvise antal af virksomheder, der - ud fra de stillede spørgsmål og deres svar - teoretisk har en god sikkerhed på de viste områder.

Området mellem de to kurver er gråzonen. Den viser det procentuelle antal virksomheder, der har eller mener at have indført sikringstiltag på området, som måske og måske ikke vil virke i den aktuelle situation.

### 2.3 Sikkerhedsniveauet i forskellige virksomhedstyper, virksomhedsstørrelse m.v.

Et spørgsmål af særlig interesse for IT-Sikkerhedsrådet har været hvilke forskelle der måtte være imellem de forskellige brancher (bl.a. ud fra et sårbarhedssynspunkt).

Til brug herfor er der foretaget en yderligere graduering på basis af "Best Quality", således at der er udregnet en talværdi for hver af deltagerne, der angiver sikringsniveauet. Herefter er resultatet beregnet for de forskellige grupperinger. Da beregningen er gennemført ens for alle, kan de anvendes til belysning af forskelle imellem de udvalgte kategorier og senere anvendes til at vurdere den reelle frem- eller tilbagegang år for år.



Gennemsnitstallet for alle virksomhederne illustreres af den røde vandrette linie.

Resultatet viser, at der er meget store forskelle imellem de forskellige brancher og inden for den enkelte branche på virksomhedsstørrelse, hvor det ikke overraskende er de mindste virksomheder, der har den dårligste sikkerhed.

Indenfor brancherne har finanssektoren altid haft ry for at have den højeste sikkerhed, men meget tyder på, at IT-servicesektoren overgår denne. Den sikkerhedsmæssigt dårligste branche er bygge- og anlægssektoren, hvor det må konstateres, at datasikkerheden ikke er højt prioriteret.

Tallene for gruppe 1 og gruppe 2 illustrerer forskellen mellem sikringsniveauet i de virksomheder der er udpeget af Danmarks Statistik og de af IT-Sikkerhedsrådet og IT- og Forskningsministeriet. Ikke overraskende er sikringsniveauet noget højere i de mere IT-tunge virksomheder.

Forskellene mellem de virksomheder der har hele eller dele af deres IT outsourcet og de der ikke har, er ikke signifikant.

Sikringsniveauet i den private sektor er lidt højere end i den offentlige.

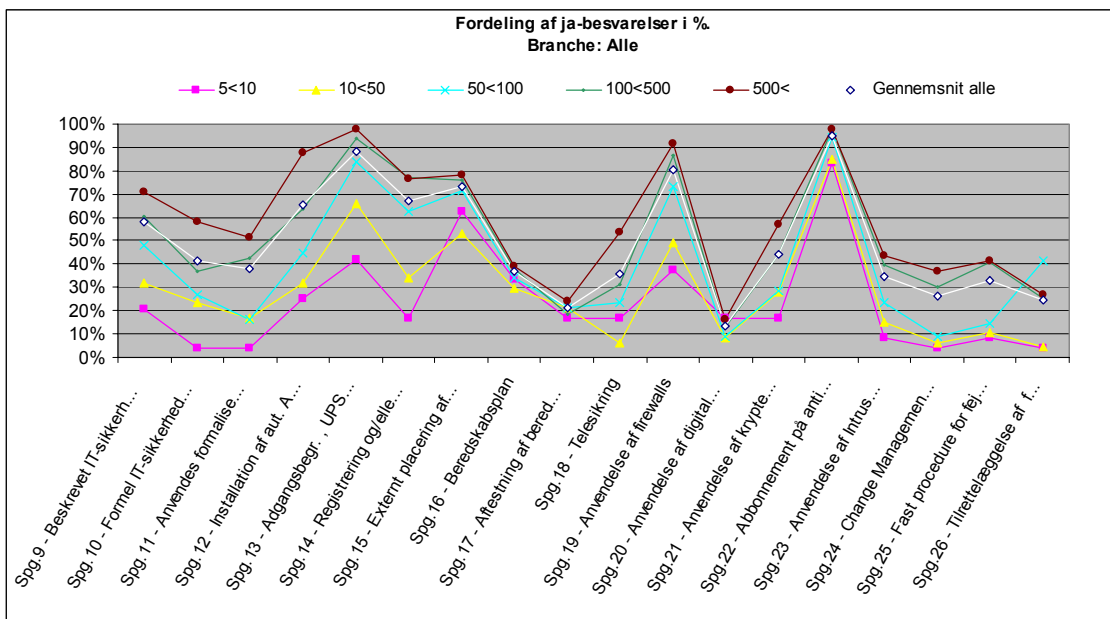
Udover fordelingen imellem de forskellige brancher indeholder grafen endvidere forskellen på sikringsniveauet mellem de forskellige virksomhedsstørrelser, og sidst men ikke mindst (de sidste to kolonner) forskellen mellem de virksomheder der har en IT-sikkerhedsfunktion og de der ikke har.

Ikke overraskende er sikkerheden væsentligt højere, når der er en IT-sikkerhedsfunktion.

### 2.4 IT-sikkerheden i forhold til virksomhedens størrelse

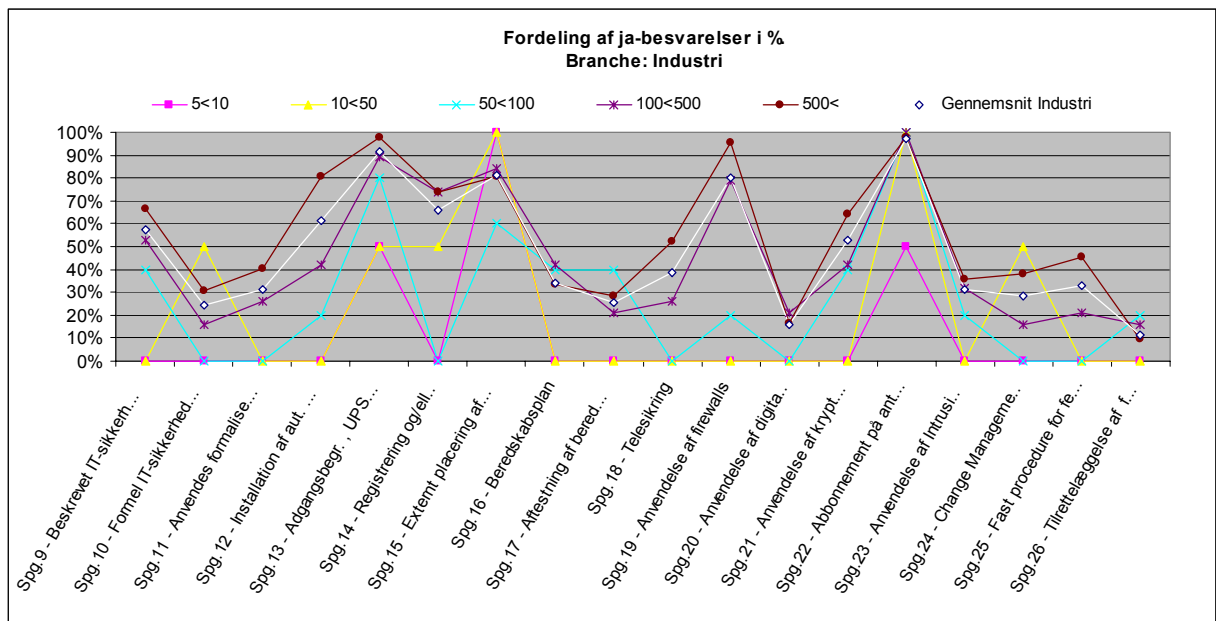
Lige så vel som der er forskelle imellem brancherne, er der forskelle indenfor den enkelte branche afhængigt af virksomhedens størrelse.

Nedenstående graf viser sikkerhedsniveauet baseret på virksomhedens størrelse:



## 2.5 IT-sikkerheden i industrien

Dette billede går igen på den enkelte branche, som dette eksempel fra industrien viser:



## 2.6 Rådets kommentarer til stamrapporteringerne

Det er et nærliggende spørgsmål at stille, om undersøgelsens resultatet generelt giver anledning til bekymring eller tilfredshed. Svaret herpå er dog vanskeligt at give. Som før nævnt findes der ingen tilsvarende undersøgelser fra andre lande og – endnu – intet historisk sammenligningsgrundlag. Derfor er det vanskeligt at udtale sig om, hvad der i forskellige henseender udgør et "gennemsnitligt" eller i øvrigt passende sikkerhedsniveau.

Med dette forbehold kan der dog være grund til at gøre nogle enkelte bemærkninger:

1. Alle danske IT-installationer har indført sikringstiltag omkring IT-anvendelsen i større eller mindre omfang.
2. Stort set alle virksomheder og institutioner har indført anti-virus beskyttelse (95%) og har i øvrigt et generelt højt sikringsniveau, når det gælder fysisk sikring og opbevaring af backup kopier eksternt. Anvendelsen af firewalls er endvidere meget høj (80%).
3. Den offentlige sektor ligger højere end den private sektor når det gælder formaliseringen af IT-sikkerhedsarbejdet - dvs. i relation til indførelse af IT-sikkerhedspolitikker, formel IT-sikkerhedsorganisation og fysisk sikring. Når man tager i betragtning, at det offentlige almindeligvis i almindelighed må arbejde under formelle rammer er dette ikke overraskende. Derimod ligger den offentlige sektor på et lavere sikringsniveau end den private sektor på alle andre områder. Dette er specielt udtryk på et område som beredskabsplaner, hvor den offentlige sektor ligger 25% lavere end den private (26% mod 46%). Tilsvarende gør sig gældende for opbevaring af eksterne backup-kopier (61% mod 82%). På baggrund af de førnævnte formaliserede rammer for sikkerhedsarbejdet i den offentlige sektor er dette lidt overraskende.
4. Et vitalt sikkerhedsmæssigt område er de såkaldte Change Management-procedurer, dvs. de foranstaltninger, den enkelte virksomhed gennemfører for at kunne sikre sig mod de risici,

der opstår under forandringsprocesser, enten udefra eller som led i ændret IT-anvendelse. Sådanne procedurer er kun indført hos ca. 26% af deltagerne. I den private sektor er der CM-procedurer i 33% af de deltagende virksomheder mod ca. 17% i de offentlige - så her er den offentlige sektor ca. 49% dårligere på et i forvejen overraskende lavt niveau. Når man vurderer disse svar må det dog tages i betragtning, at der kan være forskel på respondenternes opfattelse af, hvad en CM-procedure er, herunder om et bekræftende svar forudsætter, at sådanne procedurer er indført i form af et formaliseret sæt af regler mv.

5. Den nye lov om beskyttelse af personoplysninger trådte i kraft den 1. juli 2000 efter et langvarigt forberedelsesarbejde. På denne baggrund kan det undre, at kun ca. 24% af de deltagende virksomheder har gennemgået deres procedurer og på denne baggrund mener at kunne opfylde kravene i den nye lovgivning. I den private sektor er kun 18% klar og i den offentlige 33%. Der synes at forestå en betydelig opgave med at udbrede kendskabet til den nye lovgivning.

6. Et andet vitalt område af sikkerhedsmæssig betydning er at have styr på de uundgåelige fejl og forsinkelser i produktionen. Under 33% af deltagerne har faste procedurer for registrering heraf. Private ca. 38%, offentlige ca. 27%.

Herudover kan der være grund til at gøre nogle bemærkninger vedrørende enkelte af de sikkerhedsmæssige tiltag, der er afreporteret i undersøgelsen:

### **IT-sikkerhedspolitik, RM-procedurer, IT-sikkerhedsorganisation**

Datasikkerhed er et ledelsesansvar, men hvis ledelsen ikke formulerer målene hermed kan der være en risiko for, at de store investeringer, der gøres i indførelse af IT-sikkerhedsmæssige løsninger, ikke opnår den fornødne effekt for virksomheden. Der er ca. 40% af virksomhederne, der endnu ikke har fået udarbejdet en IT-sikkerhedspolitik.

Brug af risiko- og konsekvensanalyser (Risk Management) forinden iværksættelse af større system- og/eller teknologiadninger i virksomhederne kan medføre store besparelser og undgåelse af unødige problemer i virksomhederne.

Ser vi bort fra finanssektoren, telekommunikationssektoren og IT-servicebranchen er det mindre end 30% af deltagerne der har en formel IT-sikkerhedsorganisation. En formalisering og professionalisering af dette område vil efter Rådets opfattelse kunne spare virksomhederne for unødige omkostninger/problemer udover at have en positiv effekt på virksomhedernes drift.

### **Backup sikring**

Backup er en af de vigtigste sikringsforanstaltninger. Selvom 73% af virksomhederne opbevarer sine backup-kopier andetsteds end i den bygning, hvor det mest kritiske udstyr er placeret, medfører dette at 27% af virksomhederne ikke gør dette. Det er en billig og nem løsning af opbevare backup'er eksternt, men modstående hensyn - f.eks. vedrørende confidentialiteten af de opbevarede data - kan umiddelbart tale i modsat retning. Der synes at være behov for en nærmere vejledning om, hvorledes IT-brugeren mest effektivt og billigt sikrer sig løbende backup.

### **Beredskabsplaner**

Omkring 26% af virksomhederne i offentlige sektor og 46% af de private virksomheder udtaler, at de har beredskabsplaner. En stor del af disse bekræftelser kan hænge sammen med det store arbejde, der udførtes omkring årtusindskiftet, og der er derfor ikke vished for, at arbejdet med beredskabsplanlægningen er udtryk for en generel prioritering blandt de adspurgte. Tilbage står imidlertid, at - i bedste fald - omkring 60% af virksomheder og

institutioner i Danmark ikke har en beredskabsplan for deres IT-behandling. Dette tal finder IT-Sikkerhedsrådet betænkeligt lavt, og der kan således være behov for at synliggøre fordelene for at foretage forudgående beredskabsplanlægning blandt IT-brugerne.

### **Change Management**

Som allerede nævnt er udbredelsen af systemer til ændringshåndtering (Change Management procedurer) forbløffende lavt. Omkring 26% af de adspurgte anvender sådanne procedurer, hvor til sammenligning Firewalls har en dækning på omkring 80%. Med forbehold for, at svarene kan dække over forskellige opfattelser af de stillede spørgsmål kan der være behov for også at synliggøre denne problemstilling.

### **Lovgivningen om persondataskyttelse**

Selv om man ikke kan slutte fra det forhold, at man ikke har gennemgået sine forretningsgange og procedurer for eventuel tilpasning til den nye lov om behandling af personoplysninger, til at man nødvendigvis også overtræder denne lov, finder IT-Sikkerhedsrådet det betænkeligt, at så få virksomheder og institutioner på nuværende tidspunkt har svaret nej til spørgsmålet (24%).

### 3. Hændelsesrapporteringerne år 2000

#### 3.1 Undersøgelsen

Hændelsesrapporteringerne indberettes på skema vist i bilag 4.

Rådet har valgt at lade den første periode for rapporteringen være hele året 2000. Til sammenligning vil de efterfølgende hændelsesrapporteringer kun omfatte et halvt år ad gangen. Det forhold, at perioden omfatter et helt år, indebærer i sammenhæng med det forhold, at der ikke tidligere har været krav om eller ønske om, at skader omkring IT-behandlingen i den enkelte virksomhed har skulle registreres, at der vil være en relativt stor usikkerhed om hvilke skader der været i det forløbne år.

Når IT-Sikkerhedsrådet alligevel har valgt at gennemføre den første rapportering på helårsbasis – trods de anførte usikkerheder - skyldes det flere forhold. For det første har Rådet ønsket at vænne deltagerne i undersøgelsen til skemaerne og tilsvarende at give dem viden om, hvilke områder mv., spørgsmålene omfatter, med henblik på at kunne etablere en intern procedure for registrering heraf. For det andet har Rådet ønsket at lære af erfaringerne fra besvarelserne på de enkelte spørgsmål for bedre at kunne præcisere og afgrænse de stillede spørgsmål til brug for de efterfølgende besvarelseskemaer.

De anførte usikkerheder indebærer imidlertid, at hændelsesrapporteringerne for år 2000 bør læses med nogen større usikkerhed end den tallene for 1. halvår af 2001 må tillægges, når de fremkommer.

### 3.2 Hit-listen for uheld, skader m.v.

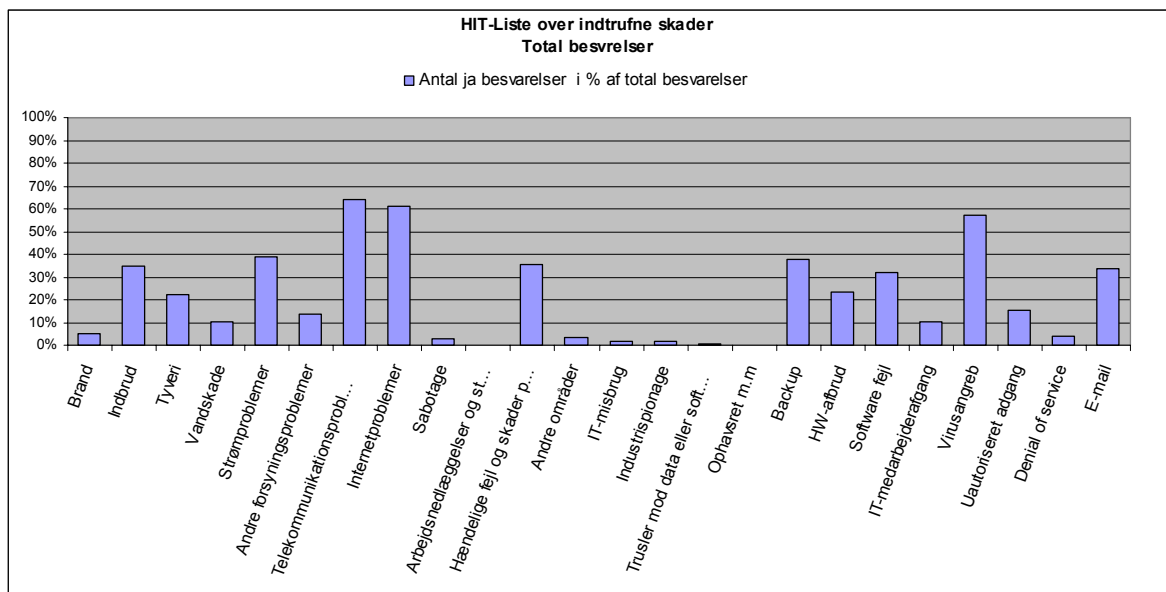
Hit-listen er baseret på de pr. 1.4.2001 indkomne besvarelser (418) og viser de uheld, skader m.v. af en vis størrelsesorden, der har ramt de deltagende installationer i løbet af år 2000. Afleveringsfristen var den 15. februar 2001.

Der er således ikke p.t. et entydigt sammenhæng til stamregistreringernes grupperinger. Det skønnes dog, at de manglende besvarelser ikke i afgørende grad vil kunne forrykke konklusionerne. En oversigt over fordelingen af de indkomne besvarelser fremgår af bilag 1.

Hit-listen baseret på antal forekomster (antal Ja-besvarelser) ser således ud:

HIT-LISTE på indtrufne skader						
418	besvarelser i alt	% af alle	Tilfælde i alt	Antal generende	Antal alvorlige	Antal katastrofale
1.	Telekommunikationsproblemer	64%	268	189	64	2
2.	Internetproblemer	61%	256	214	26	2
3.	Virusangreb	57%	239	174	43	1
4.	Strømproblemer	39%	163	120	27	1
5.	Backup	38%	157	115	27	1
6.	Hændelige fejl og skader på IT-udstyr	35%	148	97	41	3
7.	Indbrud	35%	145	100	5	1
8.	E-mail	34%	141	92	36	3
9.	Software fejl	32%	134	69	51	5
10.	HW-afbrud	23%	98	49	43	4
11.	Tyveri	22%	92	66	3	0
12.	Uautoriseret adgang	16%	65	36	7	0
13.	Andre forsyningsproblemer	14%	58	45	6	0
14.	IT-medarbejderafgang	10%	43	32	11	0
15.	Vandskade	10%	42	28	1	1
16.	Brand	5%	21	15	3	0
17.	Denial of service	4%	16	9	4	0
18.	Andre områder	3%	14	12	0	0
19.	Sabotage	3%	11	4	3	0
20.	IT-misbrug	1%	6	5	0	0
20.	Industrispionage	1%	6	4	1	0
21.	Trusler mod data eller software	0%	2	1	1	0
22.	Arbejdsnedlæggelser og strejke	0%	1	1	0	0
22.	Ophavsret m.m	0%	1	0	1	0

Grafisk ser billedet således ud:



Detaljer vedrørende de indtrufne hændelser er vist i bilag 1

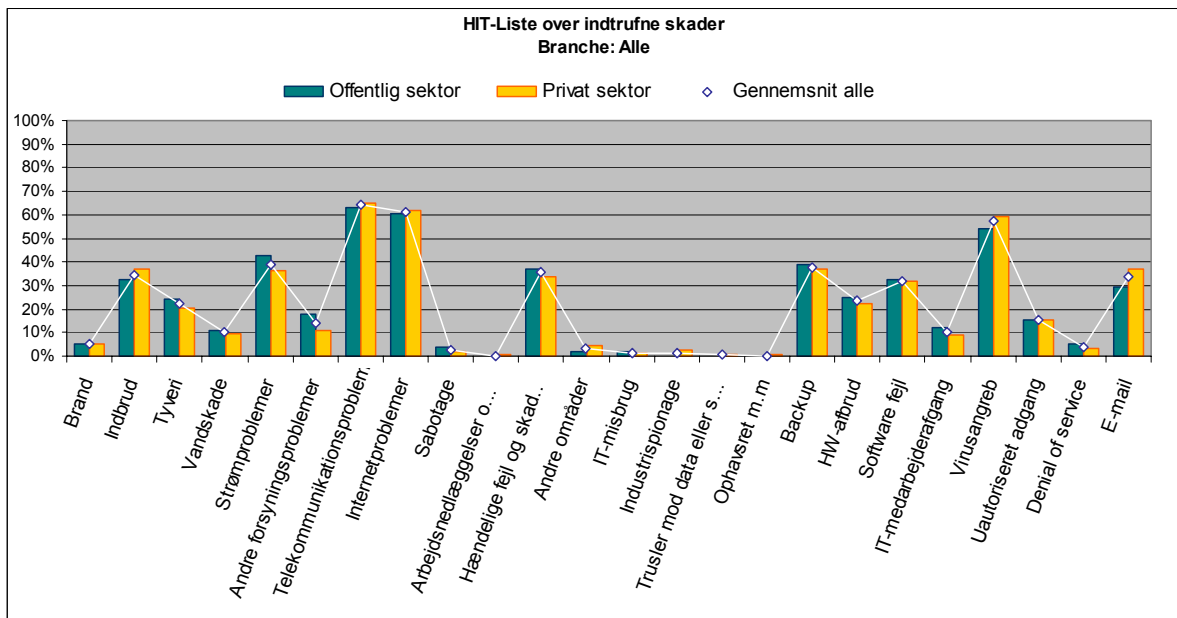
### 3.3 Hit-listen efter skadernes konsekvenser

HIT-LISTE på indtrufne skader						
418	besvarelser i alt	% af alle	Tilfælde i alt	Antal generende	Antal alvorlige	Antal katastrofale
9.	Software fejl	32%	134	69	51	5
10.	HW-afbrud	23%	98	49	43	4
6.	Hændelige fejl og skader på IT-udstyr	35%	148	97	41	3
8.	E-mail	34%	141	92	36	3
1.	Telekommunikationsproblemer	64%	268	189	64	2
2.	Internetproblemer	61%	256	214	26	2
3.	Virusangreb	57%	239	174	43	1
4.	Strømproblemer	39%	163	120	27	1
5.	Backup	38%	157	115	27	1
7.	Indbrud	35%	145	100	5	1
15.	Vandskade	10%	42	28	1	1
14.	IT-medarbejderafgang	10%	43	32	11	0
12.	Uautoriseret adgang	16%	65	36	7	0
13.	Andre forsyningsproblemer	14%	58	45	6	0
17.	Denial of service	4%	16	9	4	0
11.	Tyveri	22%	92	66	3	0
16.	Brand	5%	21	15	3	0
19.	Sabotage	3%	11	4	3	0
20.	Industrispionage	1%	6	4	1	0
21.	Trusler mod data eller software	0%	2	1	1	0
22.	Ophavsret m.m	0%	1	0	1	0
18.	Andre områder	3%	14	12	0	0
20.	IT-misbrug	1%	6	5	0	0
22.	Arbejdsnedlæggelser og strejke	0%	1	1	0	0

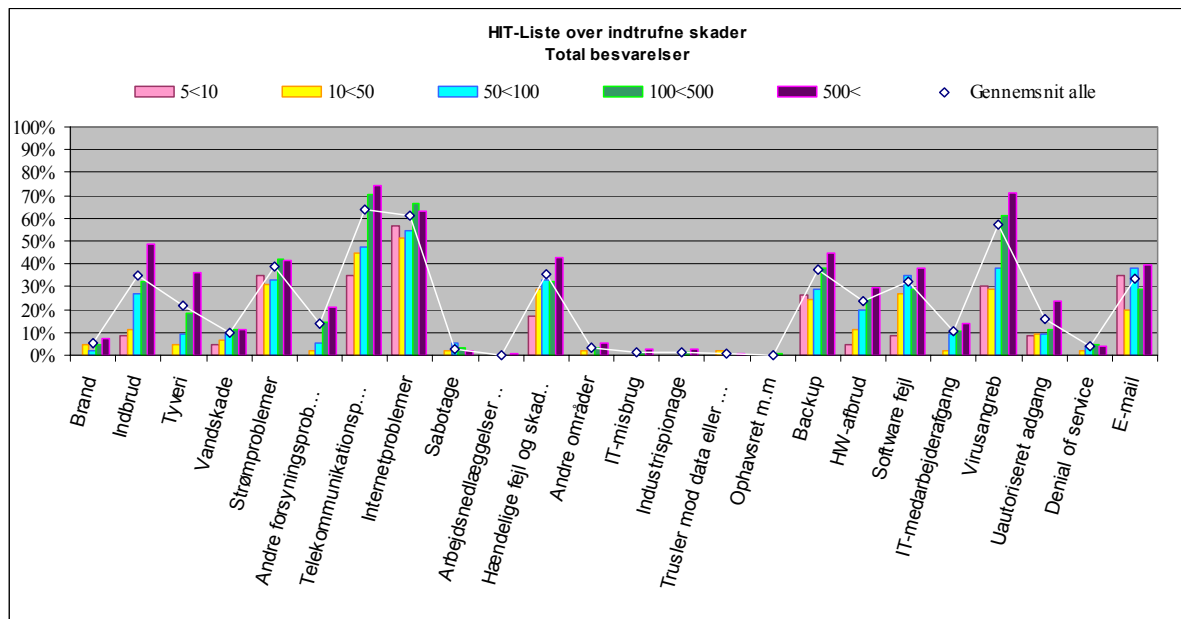
Hit-listen ser noget anderledes ud, såfremt den vises rangordnet efter de konsekvenser virksomhederne har oplevet som følge af de indtrufne hændelser/skader.

Ikke overraskende indtager software- og hardwarefejl førstepladsen. Lidt overraskende er det derimod, at e-mail problemer kan give så katastrofale konsekvenser, samt at problemer med backup og indbrud ligger så højt placeret på listen som tilfældet er.

### 3.4 Fordelingen af skader i den offentlig og den private sektor



### 3.5 Fordelingen af skader på virksomhedernes størrelse



### 3.6 Hit-listens skader fordelt på virksomheds størrelser m.v.

En fordeling af de indtrufne hændelser/skader er vist nedenfor. Tabellens venstre kolonne angiver de forskellige grupperinger, antallet af besvarelser indenfor gruppen, samt den procentuelle andel heraf. Kolonnerne markeret med 1 og 2 viser de skader, der indenfor gruppen ligger på henholdsvis 1. og 2. pladsen på gruppens hit-liste, samt antallet af krydsninger i besvarelsens JA-felt for den pågældende skade.

HÆNDELSESRREGISTRERINGER 07-04-2001			HIT-LISTE på indtrufne skader					
			1.		2.			
			%	Tifælde	%	Tifælde		
<b>Totale besvarelser</b>	<b>418</b>	<b>100%</b>	Telekommunikationsproblemer	64,1%	268	Internetproblemer	61,2%	256
5<10	23	6%	Internetproblemer	57%	13	Strømpøblemer	35%	8
10<50	45	11%	Internetproblemer	51%	23	Telekommunikationsproblemer	44%	20
50<100	55	13%	Internetproblemer	55%	30	Telekommunikationsproblemer	47%	26
100<500	124	30%	Telekommunikationsproblemer	70%	87	Internetproblemer	66%	82
500<	171	41%	Telekommunikationsproblemer	74%	127	Virusangreb	71%	122
Gruppe 1	285	68%	Telekommunikationsproblemer	62%	178	Internetproblemer	62%	176
Gruppe 2	133	32%	Virusangreb	71%	94	Telekommunikationsproblemer	68%	90
Excl. outsourcing	317	76%	Telekommunikationsproblemer	65%	207	Internetproblemer	62%	196
Offentlig sektor	186	44%	Telekommunikationsproblemer	63%	117	Internetproblemer	61%	113
Privat sektor	232	56%	Telekommunikationsproblemer	65%	151	Internetproblemer	62%	143

### 3.7 Hit-listens skader fordelt på brancher

Skemaet er opbygget på samme måde som foregående skema.

HÆNDELSESGEREGISTERINGER 07-04-2001			HIT-LISTE på indtrufne skader					
			1.		2.			
			%	Tifælde	%	Tifælde		
<b>Totale besvarelser</b>	<b>418</b>	<b>100%</b>	Telekommunikationsproblemer	64,1%	268	Internetproblemer	61,2%	256
Industri	65	16%	Telekommunikationsproblemer	72%	47	Virusangreb	69%	45
Handel	48	11%	Telekommunikationsproblemer	69%	33	Internetproblemer	67%	32
Finans	25	6%	Virusangreb	68%	17	Internetproblemer	52%	13
Transport	10	2%	Telekommunikationsproblemer	70%	7	Internetproblemer	60%	6
Energi	5	1%	Strømproblemer	80%	4	Telekommunikationsproblemer	80%	4
Telekom	3	1%	Indbrud	100%	3	Tyveri	100%	3
Byggeri	23	6%	Telekommunikationsproblemer	57%	13	Virusangreb	52%	12
IT-service	13	3%	Indbrud	69%	9	Virusangreb	69%	9
Service	27	6%	Internetproblemer	70%	19	Telekommunikationsproblemer	67%	18
Andet	13	3%	Telekommunikationsproblemer	77%	10	Internetproblemer	69%	9
Offentl. Adm. g Forv.	85	20%	Telekommunikationsproblemer	72%	61	Virusangreb	65%	55
Offentl. Pleje og sundhed	5	1%	Indbrud	60%	3	Telekommunikationsproblemer	60%	3
Offentl. Forsyning og transport	6	1%	Internetproblemer	100%	6	Virusangreb	83%	5
Offentl. Servicefunkt.	12	3%	Internetproblemer	67%	8	Telekommunikationsproblemer	58%	7
Offentl. Andet	25	6%	Telekommunikationsproblemer	68%	17	Internetproblemer	64%	16
Uddannelse	36	9%	Internetproblemer	64%	23	Virusangreb	47%	17
Sygehuse og hospitaler	17	4%	Indbrud	53%	9	Telekommunikationsproblemer	53%	9

### 3.8 Rådets kommentarer til hændelsesrapporteringerne

Hit-listen afslører en række forhold af særlig interesse:

1. Ud fra de givne besvarelser kan danske IT-installationer forvente at komme ud for 5,1 hændelser/skader en eller flere gange af betydning for IT-sikkerheden pr. år.
2. At danske virksomheder ikke kan konstatere, at de har haft besøg af hackere i det store omfang, som man måske kunne få indtryk af fra avisernes hyppige omtale af hackerproblemet. Kun en mindre del af virksomhederne har været udsat for forsøg på uautoriseret adgangsforsøg (16%).
3. Det er endvidere bemærkelsesværdigt, at ingen af de ramte virksomheder har følt konsekvenserne heraf som andet end "generende". Denne opfattelse kan tænkes at hænge sammen med en generel oplevelse af, at det ikke anses for kritisk, at oplysninger i virksomhedens IT-system kompromitteres, eller en tro på, at forsøget på indtrængen i IT-systemet ikke har ført til en sådan kompromittering eller i egentlig ødelæggelse af systemet.
4. At ikke mindre end 64% af de deltagende virksomheder havde været udsat for et eller flere telekommunikationsproblemer forekommer stærkt overraskende. Uanset om årsagen hertil er at finde i driftsproblemer hos den valgte telekommunikationsleverandør eller graveskader i kabelnettet kan der være grund til at vie dette problem særlig opmærksomhed.
5. At internetproblemer ligger næsten lige så højt er også ret overraskende. Det kan dog ikke udelukkes, at der i dette tal (61%) kan indgå nogle afledte størrelser af telekommunikationsproblemerne.
6. At en fundamental ting som strømproblemer rammer ikke mindre 39% af deltagerne kan undre i vort moderne samfund.
7. Tilsvarende gælder for backup, hvor 38% har været ramt af problemer hermed en eller flere gange. I betragtning af at dette er den mest basale sikringsforanstaltning enhver virksomhed bør kunne stole på, er tallet chokerende.

8. Det skal også bemærkes, at indbrud og tyveri af IT-udstyr rammer ikke mindre end henholdsvis 35 og 22% af de deltagende virksomheder, hvilket er tal i en størrelsesorden man svært kan forestille sig i Danmark.
9. Anledning til bekymring giver også det store antal virksomheder der har været ramt af e-mail problemer (34%).

Sammenfattende, og med forbehold for de usikkerheder, der skyldes, at de fremlagte tal udgør det første års afrapportering og derfor er behæftet med en større usikkerhed end de efterfølgende formodes at blive, må det konstateres at de væsentligste problemer, danske virksomheder oplever, er *telekommunikations- og internetproblemer, virus-problemer* og problemer i forbindelse med *hardware- og softwarefejl* samt *strømproblemer*.

### **Telekommunikation, strømforsyning og virusangreb**

Set i en overordnet samfundsmæssig ramme finder Rådet at problemerne vedrørende telekommunikation, strømforsyning og virusangreb indebærer en alvorlig svækkelse af den IT-infrastruktur, der gerne skulle være grundlaget for vort netværkssamfund. Vil Danmark være en førende IT-nation, må det anbefales, at der gøres en indsats for at reducere disse problemer væsentligt. Under sine indledende drøftelser af undersøgelsesresultaterne har Rådet allerede overvejet at sætte ind med vejledninger om sikkerhedskopiering samt en indsats vedrørende graveskader. Hertil kommer de initiativer, Rådet allerede har sat i værk, bl.a. med en vejledning om sikkerhed ved e-post og Internet-anvendelse og med en generel udredning om Danmarks Internet-relaterede sårbarhed. Rådet vil prioritere dette arbejde højest i indeværende år.

### **Problemer vedrørende backup**

Det samme gælder de afrapporterede problemer, som mange virksomheder tilsyneladende har på backup-området. Også dette område vil IT-Sikkerhedsrådet gøre til genstand for yderligere behandling i Rådet i løbet af året.

### **E-mailproblemer**

Rådet bemærker endvidere, at e-mailområdet udgør en stadig stigende del af virksomhedernes infrastruktur og kommunikationsvej, hvilket gør virksomhederne sårbare overfor forsinkelser, afbrydelser og tab af e-mails. Det må forekomme overraskende, at ikke mindre end 33% af deltagerne har været ramt heraf en eller flere gange. Besvarelserne af dette område må dog underkastes en nærmere analyse, inden Rådet kan tage yderligere skridt desangående, udover den vejledning, Rådet allerede har udsendt i marts 2001. Der er således ikke vished om, hvorvidt problemerne skyldes valget af bestemte e-mail programmer, den praktiske håndtering af programmerne eller et samspil med andre af de risikofaktorer, der kan få betydning for driftssikkerheden af et e-mail-system (strøm- og telekommunikationsnedbrud, programfejl mv.).

### **Hacking, DOS-angreb og andre retsstridige angreb**

På anden side må det forekomme glædeligt, at omfanget af hackerangreb, DOS angreb og lign. endnu ikke har nået de uoverskuelige dimensioner, som man kan få indtryk af fra pressen. Rådet vil nu foretage en nærmere undersøgelse af, hvad der kendetegner de tilfælde, hvor et ulovligt adgangsforsøg er lykkedes.

### **Fysiske indbrud**

Sidst - men ikke mindst - kan Rådet konstatere, ikke mindre end 35% af virksomhederne har været berørt af indbrud, hvor der er stjålet IT-udstyr og eller data i år 2000. Tallet gør det

nærliggende at knytte større opmærksomhed omkring mulighederne for at forebygge og forhindre tyveri.

#### **4. Det videre arbejde**

På basis af de indtil nu indkomne resultater for år 2000, har Rådet allerede indikeret at det vil tage en række initiativer i løbet af året på udvalgte områder.

Endvidere vil Rådet bearbejde de indkomne tal yderligere og sammenholde virksomhedernes sikringsniveau med de indtrufne skader, for derigennem nærmere at kunne vurdere risici, beskyttelse og i sidste ende økonomi.

Undersøgelsen fortsætter med de deltagende virksomheder året ud, idet der forventes udsendt hændelsesregistreringsskemaer for 1. og 2. halvår år 2001 i henholdsvis juni og december. Fra oktober måned vil der blive åbnet for tilgang til undersøgelsen af nye deltagere der måtte have interesse heri.

## Bilag 1

# Detaljer vedrørende de indtrufne hændelser

De efterfølgende sider indeholder nærmere informationer om de indtrufne hændelser og deres fordeling på brancher, størrelse etc.

**Spørgsmål 1. BRAND**

Har virksomheden i den forløbne periode været udsat for en eller flere brande?

<b>Brand</b>		418 besvarelser i alt	
<b>Antal Ja-svar i alt</b>		<b>21</b>	<b>5%</b>
<i>heraf</i>	<i>5&lt;10</i>	0	0%
	<i>10&lt;50</i>	2	10%
	<i>50&lt;100</i>	1	5%
	<i>100&lt;500</i>	6	29%
	<i>500&lt;</i>	12	57%
	<i>Offentlig sektor</i>	9	43%
	<i>Privat sektor</i>	12	57%
	<i>excl.outsourcing</i>	18	86%
	<i>Industri</i>	4	19%
	<i>Handel</i>	4	19%
	<i>Finans</i>	0	0%
	<i>Transport</i>	0	0%
	<i>Energi</i>	0	0%
	<i>Telekom</i>	1	5%
	<i>Byggeri</i>	1	5%
	<i>IT-service</i>	0	0%
	<i>Service</i>	0	0%
	<i>Andet</i>	2	10%
	<i>Adm og forv.</i>	2	10%
	<i>Pleje og sundhed</i>	0	0%
	<i>Forsyning og transport</i>	0	0%
	<i>Servicefunkt.</i>	2	10%
	<i>Offentl. Andet</i>	0	0%
	<i>Uddannelse</i>	2	10%
	<i>Hospital og sygehuse</i>	3	14%
	<b>I alt</b>	<b>21</b>	<b>100%</b>
<b>Antal tilfælde*</b>		<b>31</b>	
	<i>Antal tilfælde i gennemsnit</i>	1,63	
	<i>Højst antal tilfælde</i>	10	
<b>Følgeskader:</b>			
	<i>på data</i>	1	
	<i>på IT-udstyr</i>	4	
	<i>på lokaler med IT-udstyr</i>	4	
<b>Værste tilfælde forvoldte IT-stop i timer*</b>		<b>12</b>	
<b>Antal tilfælde beskrevet:</b>			
	<i>Generende</i>	15	
	<i>Alvorlige</i>	3	
	<i>Katastrofale</i>	0	

\*Af de der har angivet et præcist antal

**Spørgsmål 2: INDBRUD****Har virksomheden i den forløbne periode haft et eller flere indbrudsforsøg?**

Indbrud 418 besvarelser i alt

<b>Antal Ja-svar i alt</b>		<b>145</b>	<b>35%</b>
<i>heraf</i>	<i>5&lt;10</i>	2	1%
	<i>10&lt;50</i>	5	3%
	<i>50&lt;100</i>	15	10%
	<i>100&lt;500</i>	40	28%
	<i>500&lt;</i>	83	57%
	<i>Offentlig sektor</i>	60	41%
	<i>Privat sektor</i>	85	59%
	<i>excl.outsourcing</i>	107	74%
	<i>Industri</i>	27	19%
	<i>Handel</i>	18	12%
	<i>Finans</i>	7	5%
	<i>Transport</i>	1	1%
	<i>Energi</i>	1	1%
	<i>Telekom</i>	3	2%
	<i>Byggeri</i>	8	6%
	<i>IT-service</i>	9	6%
	<i>Service</i>	8	6%
	<i>Andet</i>	3	2%
	<i>Adm og forv.</i>	23	16%
	<i>Pleje og sundhed</i>	3	2%
	<i>Forsyning og transport</i>	0	0%
	<i>Servicefunkt.</i>	4	3%
	<i>Offentl. Andet</i>	7	5%
	<i>Uddannelse</i>	14	10%
	<i>Hospital og sygehuse</i>	9	6%
	<b>I alt</b>	<b>145</b>	<b>100%</b>

**Antal tilfælde\*** 509

Antal tilfælde i gennemsnit 3,64

Højst antal tilfælde 58

**Følgeskader:**

stjålet IT-udstyr 108

sthålet data udover det it-udstyret indholdte 6

hærværk 13

**Værste tilfælde forvoldte IT-stop i timer\*** 336**Antal tilfælde beskrevet:**

Generende 100

Alvorlige 5

Katastrofale 1

\*Af de der har angivet et præcist antal

**Spørgsmål 3: TYVERI**

Har virksomheden i den forløbne periode været udsat for tyveri af IT-udstyr og/eller data uden synlige tegn, der tyder på indbrudstyveri?

Tyveri 418 besvarelser i alt

<b>Antal Ja-svar i alt</b>	<b>92</b>	<b>22%</b>
<i>heraf</i> 5<10	0	0%
10<50	2	2%
50<100	5	5%
100<500	23	25%
500<	62	67%
Offentlig sektor	45	49%
Privat sektor	47	51%
<i>excl.outsourcing</i>	73	79%
Industri	17	18%
Handel	7	8%
Finans	6	7%
Transport	2	2%
Energi	2	2%
Telekom	3	3%
Byggeri	0	0%
IT-service	3	3%
Service	3	3%
Andet	4	4%
Adm og forv.	19	21%
Pleje og sundhed	1	1%
Forsyning og transport	3	3%
Servicefunkt.	4	4%
Offentl. Andet	3	3%
Uddannelse	10	11%
Hospital og sygehuse	5	5%
<b>I alt</b>	<b>92</b>	<b>100%</b>

**Antal tilfælde\*** **415**

Antal tilfælde i gennemsnit 4,61

Højest antal tilfælde 150

**Følgeskader:**

IT-udstyr blev stjålet **85**

Der blev stjålet (udover de i IT-udstyret indeholdte) **5**

**Værste tilfælde forvoldte IT-stop i timer\*** **72**

**Antal tilfælde beskrevet:**

Generende 66

Alvorlige 3

Katastrofale 0

\*Af de der har angivet et præcist antal

**Spørgsmål 4: VANDSKADE****Har virksomheden i den forløbne periode været udsat for vandskader?****Vandskade** 418 besvarelser i alt

<b>Antal Ja-svar i alt</b>	<b>42</b>	<b>10%</b>
<i>heraf</i> 5<10	1	2%
10<50	3	7%
50<100	5	12%
100<500	14	33%
500<	19	45%
Offentlig sektor	20	48%
Privat sektor	22	52%
<i>excl.outsourcing</i>	30	71%
Industri	9	21%
Handel	3	7%
Finans	2	5%
Transport	0	0%
Energi	1	2%
Telekom	1	2%
Byggeri	0	0%
IT-service	1	2%
Service	2	5%
Andet	3	7%
Adm og forv.	9	21%
Pleje og sundhed	1	2%
Forsyning og transport	0	0%
Servicefunkt.	1	2%
Offentl. Andet	0	0%
Uddannelse	7	17%
Hospital og sygehuse	2	5%
<b>I alt</b>	<b>42</b>	<b>100%</b>

**Antal tilfælde\*** 65

Antal tilfælde i gennemsnit 1,59

Højest antal tilfælde 8

**Følgeskader:**

IT-udstyr blev stjålet 24

Der blev stjålet (udover de i IT-udstyret indeholdte) 21

**Værste tilfælde forvoldte IT-stop i timer\*** 24**Antal tilfælde beskrevet:**

Generende 28

Alvorlige 1

Katastrofale 1

\*Af de der har angivet et præcist antal

**Spørgsmål 5: STRØMPROBLEMER**

Har virksomheden i den forløbne periode haft problemer med strømforsyningen i form af eks. strømsvingninger, lynnedslag, strømafbrydelser eller lign., der har medført problemer for IT-produktionen?

Strømproblemer		418 besvarelser i alt	
<b>Antal Ja-svar i alt</b>		<b>163</b>	<b>39%</b>
<i>heraf</i>	<i>5&lt;10</i>	8	5%
	<i>10&lt;50</i>	14	9%
	<i>50&lt;100</i>	18	11%
	<i>100&lt;500</i>	52	32%
	<i>500&lt;</i>	71	44%
<i>Offentlig sektor</i>		79	48%
<i>Privat sektor</i>		84	52%
<i>excl.outsourcing</i>		131	80%
<i>Industri</i>		22	13%
<i>Handel</i>		18	11%
<i>Finans</i>		9	6%
<i>Transport</i>		1	1%
<i>Energi</i>		4	2%
<i>Telekom</i>		1	1%
<i>Byggeri</i>		10	6%
<i>IT-service</i>		3	2%
<i>Service</i>		12	7%
<i>Andet</i>		4	2%
<i>Adm og forv.</i>		38	23%
<i>Pleje og sundhed</i>		2	1%
<i>Forsyning og transport</i>		4	2%
<i>Servicefunkt.</i>		5	3%
<i>Offentl. Andet</i>		11	7%
<i>Uddannelse</i>		11	7%
<i>Hospital og sygehuse</i>		8	5%
<b>I alt</b>		<b>163</b>	<b>100%</b>
<b>Antal tilfælde*</b>		<b>299</b>	
<i>Antal tilfælde i gennemsnit</i>		1,94	
<i>Højst antal tilfælde</i>		10	
<b>Følgeskader:</b>			
<i>Strømsvingninger der påvirkede IT-produktionen</i>		<b>37</b>	
<i>Strømafbrydelser</i>		<b>114</b>	
<i>Lynnedslag der påvirkede IT-produktionen</i>		<b>44</b>	
<b>Værste tilfælde forvoldte IT-stop i timer*</b>		<b>72</b>	
<b>Antal tilfælde beskrevet:</b>			
<i>Generende</i>		120	
<i>Alvorlige</i>		27	
<i>Katastrofale</i>		1	

\*Af de der har angivet et præcist antal

**Spørgsmål 6: ANDRE FORSYNINGER**

Har virksomheden i den forløbne periode haft andre problemer omkring forsyninger der kan påvirke IT-produktionen - eks. vand og køl?

<b>Andre forsyningsproblemer</b>		418 besvarelser i alt	
<b>Antal Ja-svar i alt</b>		<b>58</b>	<b>14%</b>
<i>heraf</i>	<i>5&lt;10</i>	0	0%
	<i>10&lt;50</i>	1	2%
	<i>50&lt;100</i>	3	5%
	<i>100&lt;500</i>	18	31%
	<i>500&lt;</i>	36	62%
	<i>Offentlig sektor</i>	33	57%
	<i>Privat sektor</i>	25	43%
	<i>excl.outsourcing</i>	48	83%
	<i>Industri</i>	12	21%
	<i>Handel</i>	3	5%
	<i>Finans</i>	3	5%
	<i>Transport</i>	0	0%
	<i>Energi</i>	1	2%
	<i>Telekom</i>	0	0%
	<i>Byggeri</i>	1	2%
	<i>IT-service</i>	1	2%
	<i>Service</i>	3	5%
	<i>Andet</i>	1	2%
	<i>Adm og forv.</i>	20	34%
	<i>Pleje og sundhed</i>	1	2%
	<i>Forsyning og transport</i>	2	3%
	<i>Servicefunkt.</i>	1	2%
	<i>Offentl. Andet</i>	4	7%
	<i>Uddannelse</i>	4	7%
	<i>Hospital og sygehuse</i>	1	2%
	<b>I alt</b>	<b>58</b>	<b>100%</b>

**Antal tilfælde\*** **81**

*Antal tilfælde i gennemsnit* 1,45

*Højst antal tilfælde* 7

**Værste tilfælde forvoldte IT-stop i timer\*** **18**

**Antal tilfælde beskrevet:**

*Generende* 45

*Alvorlige* 6

*Katastrofale* 1

\*Af de der har angivet et præcist antal

**Spørgsmål 7: TELEKOMMUNIKATIONSPROBLEMER**

**Har virksomheden i den forløbne periode haft problemer med telekommunikationslinierne der anvendes til IT-produktionen, herunder virksomhedens internetforbindelser?**

**Telekommunikationsproblemer** 418 besvarelser i alt

<b>Antal Ja-svar i alt</b>	<b>268</b>	<b>64%</b>
<i>heraf</i>		
5<10	8	3%
10<50	20	7%
50<100	26	10%
100<500	87	32%
500<	127	47%
Offentlig sektor	117	44%
Privat sektor	151	56%
<i>excl.outsourcing</i>	207	77%
Industri	47	18%
Handel	31	12%
Finans	11	4%
Transport	7	3%
Energi	4	1%
Telekom	2	1%
Byggeri	13	5%
IT-service	8	3%
Service	18	7%
Andet	10	4%
Adm og forv.	61	23%
Pleje og sundhed	3	1%
Forsyning og transport	4	1%
Servicefunkt.	7	3%
Offentl. Andet	17	6%
Uddannelse	16	6%
Hospital og sygehuse	9	3%
<b>I alt</b>	<b>268</b>	<b>100%</b>

**Antal tilfælde\*** **2633**

Antal tilfælde i gennemsnit 10,45

Højst antal tilfælde 365

**Følgeskader:**

Fejl og forsinkelser på transmissionen **114**

Leveringsproblemer med nye og/eller ændringer **63**

Afbrydelser af forbindelse **221**

**Værste tilfælde forvoldte IT-stop i timer\*** **360**

**Antal tilfælde beskrevet:**

Generende 189

Alvorlige 64

Katastrofale 2

\*Af de der har angivet et præcist antal

**Spørgsmål 8: INTERNETPROBLEMER****Har virksomheden i den forløbne periode haft problemer med adgangen til/fra internettet?**

Internetproblemer 418 besvarelser i alt

<b>Antal Ja-svar i alt</b>	<b>256</b>	<b>61%</b>
<i>heraf</i>		
5<10	13	5%
10<50	23	9%
50<100	30	12%
100<500	82	32%
500<	108	42%
<i>Offentlig sektor</i>	113	44%
<i>Privat sektor</i>	143	56%
<i>excl.outsourcing</i>	196	77%
<i>Industri</i>	43	17%
<i>Handel</i>	30	12%
<i>Finans</i>	13	5%
<i>Transport</i>	6	2%
<i>Energi</i>	3	1%
<i>Telekom</i>	1	0%
<i>Byggeri</i>	11	4%
<i>IT-service</i>	8	3%
<i>Service</i>	19	7%
<i>Andet</i>	9	4%
<i>Adm og forv.</i>	51	20%
<i>Pleje og sundhed</i>	3	1%
<i>Forsyning og transport</i>	6	2%
<i>Servicefunkt.</i>	8	3%
<i>Offentl. Andet</i>	16	6%
<i>Uddannelse</i>	23	9%
<i>Hospital og sygehuse</i>	6	2%
<b>I alt</b>	<b>256</b>	<b>100%</b>

**Antal tilfælde\* 1616**

Antal tilfælde i gennemsnit 6,76

Højst antal tilfælde 187

**Følgeskader:**

Fejl i egne internetapplikationer 72

Fejl eller nedbrud hos Internetleverandøren 185

Mangl. tilgængelighed hos samarb. partnere eller leverandør (udover internetleverandører) 80

**Værste tilfælde forvoldte IT-stop i timer\* 480****Antal tilfælde beskrevet:**

Generende 214

Alvorlige 26

Katastrofale 2

\*Af de der har angivet et præcist antal

**Spørgsmål 9: SABOTAGE**

**Har virksomheden i den forløbne periode været udsat for fysiske sabotageforsøg, hærværk eller trusler imod de fysiske IT-installationer eller lign?**

<b>Sabotage</b>		418 besvarelser i alt	
<b>Antal Ja-svar i alt</b>		<b>11</b>	<b>3%</b>
<i>heraf</i>	<i>5&lt;10</i>	0	0%
	<i>10&lt;50</i>	1	9%
	<i>50&lt;100</i>	3	27%
	<i>100&lt;500</i>	4	36%
	<i>500&lt;</i>	3	27%
	<i>Offentlig sektor</i>	7	64%
	<i>Privat sektor</i>	4	36%
	<i>excl.outsourcing</i>	8	73%
	<i>Industri</i>	0	0%
	<i>Handel</i>	1	9%
	<i>Finans</i>	0	0%
	<i>Transport</i>	0	0%
	<i>Energi</i>	0	0%
	<i>Telekom</i>	1	9%
	<i>Byggeri</i>	0	0%
	<i>IT-service</i>	0	0%
	<i>Service</i>	0	0%
	<i>Andet</i>	2	18%
	<i>Adm og forv.</i>	1	9%
	<i>Pleje og sundhed</i>	0	0%
	<i>Forsyning og transport</i>	1	9%
	<i>Servicefunkt.</i>	0	0%
	<i>Offentl. Andet</i>	0	0%
	<i>Uddannelse</i>	5	45%
	<i>Hospital og sygehuse</i>	0	0%
	<b>I alt</b>	<b>11</b>	<b>100%</b>

**Antal tilfælde\*** **16**

*Antal tilfælde i gennemsnit* 1,78

*Højst antal tilfælde* 5

**Form for sabotage:**

*Fysiske sabotageforsøg* **3**

*Hærværk* **5**

*Trusler der tages alvorligt* **1**

**Værste tilfælde forvoldte IT-stop i timer\*** **0**

**Antal tilfælde beskrevet:**

*Generende* 4

*Alvorlige* 3

*Katastrofale* 0

\*Af de der har angivet et præcist antal

**Spørgsmål 10: ARBEJDSNEDLÆGGELSE OG STREJKE**

**Har virksomheden i den forløbne periode været ramt af arbejdsnedlæggelser, strejke eller anden afbrydelse af arbejdet forårsaget af virksomhedens IT-medarbejdere?**

**Arbejdsnedlæggelser og strejke** 418 besvarelser i alt

<b>Antal Ja-svar i alt</b>	<b>1</b>	<b>0,24%</b>
<i>heraf</i> 5<10	0	0%
10<50	0	0%
50<100	0	0%
100<500	0	0%
500<	1	100%
Offentlig sektor	0	0%
Privat sektor	1	100%
excl.outsourcing	1	100%
Industri	0	0%
Handel	1	100%
Finans	0	0%
Transport	0	0%
Energi	0	0%
Telekom	0	0%
Byggeri	0	0%
IT-service	0	0%
Service	0	0%
Andet	0	0%
Adm og forv.	0	0%
Pleje og sundhed	0	0%
Forsyning og transport	0	0%
Servicefunkt.	0	0%
Offentl. Andet	0	0%
Uddannelse	0	0%
Hospital og sygehuse	0	0%
<b>I alt</b>	<b>1</b>	<b>100%</b>

**Antal tilfælde\*** 1

Antal tilfælde i gennemsnit 1,00

Højst antal tilfælde 1

**Form for strejke:**

Massive sygemeldinger 0

Ulovlige arbejdsnedlæggelser 0

Strejker 1

**Værste tilfælde forvoldte IT-stop i timer\*** 0

**Antal tilfælde beskrevet:**

Generende 1

Alvorlige 0

Katastrofale 0

\*Af de der har angivet et præcist antal

**Spørgsmål 11: HÆNDELIGE FEJL OG SKADER PÅ IT-UDSTYR**

**Har virksomheden i den forløbne periode været ramt af hændelige fysiske skader og fysiske fejl på IT-udstyr, der har medført IT-stop?**

Hændelige fejl og skader på IT-udstyr 418 besvarelser i alt

<b>Antal Ja-svar i alt</b>	<b>148</b>	<b>35%</b>
<i>heraf</i> 5<10	4	3%
10<50	13	9%
50<100	18	12%
100<500	40	27%
500<	73	49%
Offentlig sektor	69	47%
Privat sektor	79	53%
<i>excl.outsourcing</i>	111	75%
Industri	26	18%
Handel	17	11%
Finans	7	5%
Transport	1	1%
Energi	2	1%
Telekom	0	0%
Byggeri	5	3%
IT-service	3	2%
Service	10	7%
Andet	8	5%
Adm og forv.	31	21%
Pleje og sundhed	1	1%
Forsyning og transport	3	2%
Servicefunkt.	4	3%
Offentl. Andet	9	6%
Uddannelse	14	9%
Hospital og sygehuse	7	5%
<b>I alt</b>	<b>148</b>	<b>100%</b>

**Antal tilfælde\*** **494**

Antal tilfælde i gennemsnit 3,63

Højest antal tilfælde 50

**Form for hændelige fejl**

Computere (servere, main-frames etc.) **118**

Netværk (kabler, krydsfelter etc.) **71**

Egne forsyningsenheder (transforamtorer, køleudstyr etc.) **19**

**Værste tilfælde forvoldte IT-stop i timer\*** **336**

**Antal tilfælde beskrevet:**

Generende 97

Alvorlige 41

Katastrofale 3

\*Af de der har angivet et præcist antal

**Spørgsmål 12: ANDRE OMRÅDER**

**Har virksomheden i den forløbne periode været udsat for klager fra medarbejdere, tillidsrepræsentanter, fagforeninger eller andre, vedrørende virksomhedens anvendelse af TV-overvågning, registrering af internetanvendelse eller registrering af e-mails?**

Andre områder (klager fra medarb., fagforeninger etc.) 418 besvarelser i alt

<b>Antal Ja-svar i alt</b>		<b>14</b>	<b>3%</b>
<i>heraf</i>	5<10	0	0%
	10<50	1	7%
	50<100	0	0%
	100<500	4	29%
	500<	9	64%
	Offentlig sektor	3	21%
	Privat sektor	11	79%
	<i>excl. outsourcing</i>	10	71%
	Industri	5	36%
	Handel	3	21%
	Finans	2	14%
	Transport	0	0%
	Energi	0	0%
	Telekom	0	0%
	Byggeri	0	0%
	IT-service	1	7%
	Service	0	0%
	Andet	0	0%
	Adm og forv.	1	7%
	Pleje og sundhed	0	0%
	Forsyning og transport	0	0%
	Servicefunkt.	0	0%
	Offentl. Andet	1	7%
	Uddannelse	0	0%
	Hospital og sygehuse	1	7%
	<b>I alt</b>	<b>14</b>	<b>100%</b>

**Antal tilfælde\*** **82**

Antal tilfælde i gennemsnit 5,86  
Højst antal tilfælde 50

**Arsager for klager**

TV-overvågning **5**  
Internetanvendelse **4**  
Ind- og udgående e-mails **11**

**Antal tilfælde beskrevet:**

Generende 12  
Alvorlige 0  
Katastrofale 0

\*Af de der har angivet et præcist antal

**Spørgsmål 13: IT-MISBRUG**

**Har virksomheden i den forløbne periode været udsat for IT-misbrug af økonomisk karakter?**

IT-misbrug		418 besvarelser i alt	
<b>Antal Ja-svar i alt</b>		<b>6</b>	<b>1%</b>
<i>heraf</i>			
	5<10	0	0%
	10<50	0	0%
	50<100	0	0%
	100<500	2	33%
	500<	4	67%
	Offentlig sektor	3	50%
	Privat sektor	3	50%
	<i>excl.outsourcing</i>	4	67%
	Industri	1	17%
	Handel	1	17%
	Finans	0	0%
	Transport	0	0%
	Energi	0	0%
	Telekom	1	17%
	Byggeri	0	0%
	IT-service	0	0%
	Service	0	0%
	Andet	0	0%
	Adm og forv.	3	50%
	Pleje og sundhed	0	0%
	Forsyning og transport	0	0%
	Servicefunkt.	0	0%
	Offentl. Andet	0	0%
	Uddannelse	0	0%
	Hospital og sygehuse	0	0%
	<b>I alt</b>	<b>6</b>	<b>100%</b>

**Antal tilfælde\*** **10**

Antal tilfælde i gennemsnit 1,67  
Højest antal tilfælde 3

**Form for IT-misbrug:**

	Mistanke	Bevis	Mistanke om intern involv.
Uautoriseret salg	0	0	0
IT-bedrageri	0	2	1
Manipulation af data	2	2	0
Bevidst sletning af data	0	1	0
Andet	0	1	0

**Antal tilfælde beskrevet:**

Generende	5
Alvorlige	0
Katastrofale	0

\*Af de der har angivet et præcist antal

**Spørgsmål 14: INDUSTRIESPIONAGE**

**Har virksomheden i den forløbne periode haft mistanke om eller været udsat for industrispionage eller bevidst afsløring af data til uvedkommende?**

Industrispionage		418 besvarelser i alt	
<b>Antal Ja-svar i alt</b>		<b>6</b>	<b>1%</b>
<i>heraf</i>			
5<10		0	0%
10<50		0	0%
50<100		0	0%
100<500		2	33%
500<		4	67%
Offentlig sektor		0	0%
Privat sektor		6	100%
<i>excl.outsourcing</i>		4	67%
Industri		3	50%
Handel		0	0%
Finans		1	17%
Transport		1	17%
Energi		0	0%
Telekom		1	17%
Byggeri		0	0%
IT-service		0	0%
Service		0	0%
Andet		0	0%
Adm og forv.		0	0%
Pleje og sundhed		0	0%
Forsyning og transport		0	0%
Servicefunkt.		0	0%
Offentl. Andet		0	0%
Uddannelse		0	0%
Hospital og sygehuse		0	0%
<b>I alt</b>		<b>6</b>	<b>100%</b>

<b>Antal tilfælde*</b>	<b>7</b>
Antal tilfælde i gennemsnit	1,17
Højest antal tilfælde	2

**Form for spionage**

	Mistanke	Bevis
Industrispionage fra fremmede nationer	0	0
Industri spionage fra konkurrenter	3	0
Industrispionage fra andre	3	0
Bevidst afsløring af data	2	0

**Antal tilfælde beskrevet:**

Generende	4
Alvorlige	1
Katastrofale	0

\*Af de der har angivet et præcist antal

**Spørgsmål 15. TRUSLER MOD DATA ELLER SOFTWARE**

Har virksomheden i den forløbne periode været udsat for afpresning ved hjælp af trusler rettet mod virksomhedens data eller software?

Trusler mod data eller software 418 besvarelser i alt

<b>Antal Ja-svar i alt</b>		<b>2</b>	<b>0%</b>
<i>heraf</i>	<i>5&lt;10</i>	0	0%
	<i>10&lt;50</i>	1	50%
	<i>50&lt;100</i>	0	0%
	<i>100&lt;500</i>	0	0%
	<i>500&lt;</i>	1	50%
	<i>Offentlig sektor</i>	0	0%
	<i>Privat sektor</i>	2	100%
	<i>excl.outsourcing</i>	2	100%
	<i>Industri</i>	1	50%
	<i>Handel</i>	1	50%
	<i>Finans</i>	0	0%
	<i>Transport</i>	0	0%
	<i>Energi</i>	0	0%
	<i>Telekom</i>	0	0%
	<i>Byggeri</i>	0	0%
	<i>IT-service</i>	0	0%
	<i>Service</i>	0	0%
	<i>Andet</i>	0	0%
	<i>Adm og forv.</i>	0	0%
	<i>Pleje og sundhed</i>	0	0%
	<i>Forsyning og transport</i>	0	0%
	<i>Servicefunkt.</i>	0	0%
	<i>Offentl. Andet</i>	0	0%
	<i>Uddannelse</i>	0	0%
	<i>Hospital og sygehuse</i>	0	0%
	<b>I alt</b>	<b>2</b>	<b>100%</b>

**Antal tilfælde\*** 2

*Antal tilfælde i gennemsnit* 0

*Højest antal tilfælde* 0

**Form for trusler:**

*Truslerne er blevet effektueret* 0

*Truslerne er stadig aktive* 1

**Antal tilfælde beskrevet:**

*Generende* 1

*Alvorlige* 0

*Katastrofale* 1

\*Af de der har angivet et præcist antal

**Spørgsmål 16: OPHAVSRET M.M.**

Har virksomheden i den forløbne periode været sigtet, anklaget eller været genstand for søgsmål vedrørende ophavsret, markedsføring, straffelovens bestemmelser vedr. IT-kriminalitet, mønsterbeskyttelse (relateret til IT-anvendelsen), patentkrænkelser eller har virksomheden anmeldt/rejst sag mod andre desangående?

Ophavsret		418 besvarelser i alt	
<b>Antal Ja-svar i alt</b>		<b>1</b>	<b>0,24%</b>
<i>heraf</i>			
5<10		0	0%
10<50		0	0%
50<100		0	0%
100<500		1	100%
500<		0	0%
Offentlig sektor		0	0%
Privat sektor		1	100%
<i>excl.outsourcing</i>		1	100%
Industri		0	0%
Handel		0	0%
Finans		0	0%
Transport		0	0%
Energi		0	0%
Telekom		0	0%
Byggeri		0	0%
IT-service		0	0%
Service		1	100%
Andet		0	0%
Adm og forv.		0	0%
Pleje og sundhed		0	0%
Forsyning og transport		0	0%
Servicefunkt.		0	0%
Offentl. Andet		0	0%
Uddannelse		0	0%
Hospital og sygehuse		0	0%
<b>I alt</b>		<b>1</b>	<b>100%</b>

<b>Antal tilfælde*</b>	<b>1</b>
Antal tilfælde i gennemsnit	0,00
Højest antal tilfælde	0

**Form for tilfælde:**

	Virksomheden sigtet for/sagsøgt	Virksomheden har anmeldt/rejst sag an mod
Ophavsret	1	0
Markedsføringsloven	0	0
Straffeloven	0	0
Mønsterbeskyttelse	0	0
Patentloven	0	0

**Antal tilfælde beskrevet:**

Generende	0
Alvorlige	1
Katastrofale	0

**Spørgsmål 17: BACKUP**

**Har virksomheden i den forløbne periode haft problemer med anvendelsen af backup af data og/eller programmer?**

<b>Backup</b>		418 besvarelser i alt	
<b>Antal Ja-svar i alt</b>		<b>157</b>	<b>38%</b>
<i>heraf</i>	<i>5&lt;10</i>	6	4%
	<i>10&lt;50</i>	11	7%
	<i>50&lt;100</i>	16	10%
	<i>100&lt;500</i>	47	30%
	<i>500&lt;</i>	77	49%
	<i>Offentlig sektor</i>	72	46%
	<i>Privat sektor</i>	85	54%
	<i>excl.outsourcing</i>	124	79%
	<i>Industri</i>	27	17%
	<i>Handel</i>	18	11%
	<i>Finans</i>	8	5%
	<i>Transport</i>	2	1%
	<i>Energi</i>	2	1%
	<i>Telekom</i>	2	1%
	<i>Byggeri</i>	2	1%
	<i>IT-service</i>	5	3%
	<i>Service</i>	13	8%
	<i>Andet</i>	6	4%
	<i>Adm og forv.</i>	40	25%
	<i>Pleje og sundhed</i>	3	2%
	<i>Forsyning og transport</i>	1	1%
	<i>Servicefunkt.</i>	3	2%
	<i>Offentl. Andet</i>	11	7%
	<i>Uddannelse</i>	8	5%
	<i>Hospital og sygehuse</i>	6	4%
	<b>I alt</b>	<b>157</b>	<b>100%</b>
<b>Antal tilfælde*</b>		<b>1116</b>	
	<i>Antal tilfælde i gennemsnit</i>	7,44	
	<i>Højst antal tilfælde</i>	365	
<b>Værste tilfælde forvoldte IT-stop i timer*</b>		150	
<b>Antal tilfælde beskrevet:</b>			
	<i>Generende</i>	115	
	<i>Alvorlige</i>	27	
	<i>Katastrofale</i>	1	

\*Af de der har angivet et præcist antal

**Spørgsmål 18: HARDWARE AFBRUD**

**Har virksomheden i den forløbne periode haft betydelige afbrud i IT-produktionen som følge af fejl i IT-udstyr (hardwaren)?**

**HW-afbrud** 418 besvarelser i alt

<b>Antal Ja-svar i alt</b>	<b>98</b>	<b>23%</b>
<i>heraf</i> 5<10	1	1%
10<50	5	5%
50<100	11	11%
100<500	30	31%
500<	51	52%
Offentlig sektor	46	47%
Privat sektor	52	53%
<i>excl. outsourcing</i>	75	77%
Industri	18	18%
Handel	11	11%
Finans	4	4%
Transport	2	2%
Energi	2	2%
Telekom	2	2%
Byggeri	1	1%
IT-service	3	3%
Service	5	5%
Andet	4	4%
Adm og forv.	24	24%
Pleje og sundhed	3	3%
Forsyning og transport	0	0%
Servicefunkt.	2	2%
Offentl. Andet	4	4%
Uddannelse	6	6%
Hospital og sygehuse	7	7%
<b>I alt</b>	<b>98</b>	<b>100%</b>

**Antal tilfælde\*** 275

Antal tilfælde i gennemsnit 2,86

Højst antal tilfælde 22

**Værste tilfælde forvoldte IT-stop i timer\*** 120

**Antal tilfælde beskrevet:**

Generende 49

Alvorlige 43

Katastrofale 4

\*Af de der har angivet et præcist antal

**Spørgsmål 19: SOFTWAREFEJL**

**Har virksomheden i den forløbne periode haft betydelige afbrud eller væsentlige fejl i IT-produktionen som følge af softwareproblemer?**

<b>Softwarefejl</b>		418 besvarelser i alt	
<b>Antal Ja-svar i alt</b>		<b>134</b>	<b>32%</b>
<i>heraf</i>	<i>5&lt;10</i>	2	1%
	<i>10&lt;50</i>	12	9%
	<i>50&lt;100</i>	19	14%
	<i>100&lt;500</i>	36	27%
	<i>500&lt;</i>	65	49%
	<i>Offentlig sektor</i>	60	45%
	<i>Privat sektor</i>	74	55%
	<i>excl.outsourcing</i>	106	79%
	<i>Industri</i>	22	16%
	<i>Handel</i>	9	7%
	<i>Finans</i>	11	8%
	<i>Transport</i>	3	2%
	<i>Energi</i>	2	1%
	<i>Telekom</i>	3	2%
	<i>Byggeri</i>	5	4%
	<i>IT-service</i>	6	4%
	<i>Service</i>	9	7%
	<i>Andet</i>	4	3%
	<i>Adm og forv.</i>	26	19%
	<i>Pleje og sundhed</i>	3	2%
	<i>Forsyning og transport</i>	3	2%
	<i>Servicefunkt.</i>	5	4%
	<i>Offentl. Andet</i>	9	7%
	<i>Uddannelse</i>	10	7%
	<i>Hospital og sygehuse</i>	4	3%
	<b>I alt</b>	<b>134</b>	<b>100%</b>
<b>Antal tilfælde*</b>		<b>728</b>	
	<i>Antal tilfælde i gennemsnit</i>	6,12	
	<i>Højst antal tilfælde</i>	52	
<b>Software fejl i:</b>			
	<i>Styresystem</i>	<b>46</b>	
	<i>Standardapplikationer (indkøbte/lejede/leasede)</i>	<b>90</b>	
	<i>Egne udviklede applikationer</i>	<b>40</b>	
<b>Værste tilfælde forvoldte IT-stop i timer*</b>		<b>336</b>	
<b>Antal tilfælde beskrevet:</b>			
	<i>Generende</i>	69	
	<i>Alvorlige</i>	51	
	<i>Katastrofale</i>	5	

\*Af de der har angivet et præcist antal

**Spørgsmål 20: IT MEDARBEJDERAFGANG**

**Har virksomheden i den forløbne periode mistet IT-medarbejdere i et efter virksomhedens opfattelse for stort antal?**

IT-medarbejderafgang		418 besvarelser i alt	
<b>Antal Ja-svar i alt</b>		<b>43</b>	<b>10%</b>
<i>heraf</i>	<i>5&lt;10</i>	0	0%
	<i>10&lt;50</i>	1	2%
	<i>50&lt;100</i>	5	12%
	<i>100&lt;500</i>	13	30%
	<i>500&lt;</i>	24	56%
	<i>Offentlig sektor</i>	23	53%
	<i>Privat sektor</i>	20	47%
	<i>excl.outsourcing</i>	33	77%
	<i>Industri</i>	5	12%
	<i>Handel</i>	1	2%
	<i>Finans</i>	4	9%
	<i>Transport</i>	2	5%
	<i>Energi</i>	2	5%
	<i>Telekom</i>	0	0%
	<i>Byggeri</i>	2	5%
	<i>IT-service</i>	0	0%
	<i>Service</i>	3	7%
	<i>Andet</i>	1	2%
	<i>Adm og forv.</i>	13	30%
	<i>Pleje og sundhed</i>	0	0%
	<i>Forsyning og transport</i>	2	5%
	<i>Servicefunkt.</i>	2	5%
	<i>Offentl. Andet</i>	2	5%
	<i>Uddannelse</i>	2	5%
	<i>Hospital og sygehuse</i>	2	5%
	<b>I alt</b>	<b>43</b>	<b>100%</b>

**Antal tilfælde\*** **43**

**Antal tilfælde af IT-medarbejderafgang i %-del af IT-medarbejdere :**

	10<15%	15<20%	20>25%	Mere
<i>5&lt;10</i>	0	0	0	0
<i>10&lt;50</i>	0	0	0	0
<i>50&lt;100</i>	0	1	0	4
<i>100&lt;501</i>	3	2	2	5
<i>500&lt;</i>	10	8	5	3
<i>Offentlig sektor</i>	5	6	3	10
<i>Privat sektor</i>	8	5	4	2
<b>I alt</b>	<b>13</b>	<b>11</b>	<b>7</b>	<b>12</b>

**Antal tilfælde beskrevet:**

<i>Generende</i>	32
<i>Alvorlige</i>	11
<i>Katastrofale</i>	0

\*Af de der har angivet et præcist antal

**Spørgsmål 21: VIRUSANGREB****Er virksomheden i den forløbne periode blevet angrebet og inficeret af pc-virus, orme, trojanske heste m.m.?**

Virus angreb		418 besvarelser i alt	
<b>Antal Nej-svar i alt:</b>		<b>167</b>	<b>40%</b>
<b>Antal Ved ikke- svar i alt</b>		<b>11</b>	<b>3%</b>
<b>Antal Ja-svar i alt</b>		<b>239</b>	<b>57%</b>
heraf	5<10	7	3%
	10<50	13	5%
	50<100	21	9%
	100<500	76	32%
	500<	122	51%
Offentlig sektor		101	42%
Privat sektor		138	58%
excl.outsourcing		187	78%
Industri		45	19%
Handel		26	11%
Finans		17	7%
Transport		6	3%
Energi		3	1%
Telekom		2	1%
Byggeri		12	5%
IT-service		9	4%
Service		13	5%
Andet		5	2%
Adm og forv.		55	23%
Pleje og sundhed		0	0%
Forsyning og transport		5	2%
Servicefunkt.		5	2%
Offentl. Andet		10	4%
Uddannelse		17	7%
Hospital og sygehuse		9	4%
<b>I alt</b>		<b>239</b>	<b>100%</b>

**Antal tilfælde\*** **11.281**

Antal tilfælde i gennemsnit 48,42

Højst antal tilfælde 8.096

**Anvendt tid til bekæmpelse og opretning\***

- Samlet anvendt tid til bekæmpelse og opretning af alle viruskader på i alt ca. Person dage: 2208

Højst tilfælde af anvendt person dage på ovennævnte: 300

- I værre tilfælde anvendes til opretning i alt ca. Person dage: 747

Højst tilfælde af anvendt person dage på ovennævnte: 55

**Værste tilfælde af driftsproblemer i kalenderdage\*** **30**

**Antal tilfælde beskrevet:**

Generende 174

Alvorlige 43

Katastrofale 1

\*Af de der har angivet et præcist antal

**Spørgsmål 22: UAUTORISERET ADGANG**

**Har virksomheden i den forløbne periode været udsat for forsøg på at opnå uautoriseret adgang til systemer eller data via internettet?**

Uautoriseret adgang		418 besvarelser i alt	
<b>Antal Nej-svar i alt:</b>		<b>262</b>	<b>63%</b>
<b>Antal Ved ikke- svar i alt</b>		<b>92</b>	<b>22%</b>
<b>Antal Ja-svar i alt</b>		<b>65</b>	<b>16%</b>
<i>heraf</i>	<i>5&lt;10</i>	2	3%
	<i>10&lt;50</i>	4	6%
	<i>50&lt;100</i>	5	8%
	<i>100&lt;500</i>	14	22%
	<i>500&lt;</i>	40	62%
	<i>Offentlig sektor</i>	29	45%
	<i>Privat sektor</i>	36	55%
	<i>excl.outsourcing</i>	52	80%
	<i>Industri</i>	11	17%
	<i>Handel</i>	6	9%
	<i>Finans</i>	3	5%
	<i>Transport</i>	0	0%
	<i>Energi</i>	0	0%
	<i>Telekom</i>	2	3%
	<i>Byggeri</i>	2	3%
	<i>IT-service</i>	6	9%
	<i>Service</i>	5	8%
	<i>Andet</i>	1	2%
	<i>Adm og forv.</i>	18	28%
	<i>Pleje og sundhed</i>	0	0%
	<i>Forsyning og transport</i>	1	2%
	<i>Servicefunkt.</i>	1	2%
	<i>Offentl. Andet</i>	2	3%
	<i>Uddannelse</i>	6	9%
	<i>Hospital og sygehuse</i>	1	2%
	<b>I alt</b>	<b>65</b>	<b>100%</b>

**Antal tilfælde\*** **12.158**

*Antal tilfælde i gennemsnit* 217,11

*Højst antal tilfælde* 5.000

**Antal tilfælde hvor det opdagedes og afvistes inden indtrængning\***

- *Samlet tilfælde i alt* 11.785

- *Samlet antal vellykket tilfælde* 10

**I det værste tilfælde anvendtes i alt persondage til efterforskning og udbredning** **40**

**Antal tilfælde beskrevet:**

*Generende* 36

*Alvorlige* 7

*Katastrofale* 0

\*Af de der har angivet et præcist antal

**Spørgsmål 23: DENIAL OF SERVICES**

**Har virksomheden i den forløbne periode været udsat for ude-af-drift angreb (denial-of-service attacks)?**

<b>Denial of service</b>		418 besvarelser i alt	
<b>Antal Nej-svar i alt:</b>		<b>366</b>	<b>88%</b>
<b>Antal Ved ikke- svar i alt</b>		<b>35</b>	<b>8%</b>
<b>Antal Ja-svar i alt</b>		<b>16</b>	<b>4%</b>
<i>heraf</i>			
5<10		0	0%
10<50		1	6%
50<100		2	13%
100<500		6	38%
500<		7	44%
<i>Offentlig sektor</i>		9	56%
<i>Privat sektor</i>		7	44%
<i>excl.outsourcing</i>		12	75%
<i>Industri</i>		1	6%
<i>Handel</i>		0	0%
<i>Finans</i>		0	0%
<i>Transport</i>		0	0%
<i>Energi</i>		0	0%
<i>Telekom</i>		0	0%
<i>Byggeri</i>		1	6%
<i>IT-service</i>		2	13%
<i>Service</i>		1	6%
<i>Andet</i>		2	13%
<i>Adm og forv.</i>		4	25%
<i>Pleje og sundhed</i>		0	0%
<i>Forsyning og transport</i>		0	0%
<i>Servicefunkt.</i>		0	0%
<i>Offentl. Andet</i>		0	0%
<i>Uddannelse</i>		4	25%
<i>Hospital og sygehuse</i>		1	6%
<b>I alt</b>		<b>16</b>	<b>100%</b>
<b>Antal tilfælde*</b>		<b>78</b>	
<i>Antal tilfælde i gennemsnit</i>		6,00	
<i>Højst antal tilfælde</i>		50	
<b>Værste tilfælde forvoldte IT-stop i timer*</b>		<b>48</b>	
<b>Antal tilfælde beskrevet:</b>			
<i>Generende</i>		9	
<i>Alvorlige</i>		4	
<i>Katastrofale</i>		0	

\*Af de der har angivet et præcist antal

**Spørgsmål 24: E-MAIL**

**Har virksomheden i den forløbne periode været udsat for problemer med virksomhedens e-mail systemer, der har medført tab af e-mails eller større forsinkelser og/eller driftsstop?**

Email	418 besvarelser i alt	
<b>Antal Nej-svar i alt:</b>	<b>267</b>	<b>64%</b>
<b>Antal Ved ikke- svar i alt</b>	<b>10</b>	<b>2%</b>
<b>Antal Ja-svar i alt</b>	<b>141</b>	<b>34%</b>
<i>heraf</i>		
5<10	8	6%
10<50	9	6%
50<100	21	15%
100<500	36	26%
500<	67	48%
Offentlig sektor	55	39%
Privat sektor	86	61%
excl.outsourcing	111	79%
Industri	22	16%
Handel	22	16%
Finans	7	5%
Transport	2	1%
Energi	1	1%
Telekom	1	1%
Byggeri	5	4%
IT-service	7	5%
Service	13	9%
Andet	6	4%
Adm og forv.	26	18%
Pleje og sundhed	1	1%
Forsyning og transport	3	2%
Servicefunkt.	5	4%
Offentl. Andet	7	5%
Uddannelse	11	8%
Hospital og sygehuse	2	1%
<b>I alt</b>	<b>141</b>	<b>100%</b>
<b>Antal tilfælde*</b>	<b>50.721</b>	
Antal tilfælde i gennemsnit	372,95	
Højst antal tilfælde	50.100	
<b>Form for email problemer</b>		
større forsinkelser	<b>83</b>	
tab af mails i ukendt / større antal	<b>50</b>	
driftsstop	<b>47</b>	
<b>Værste tilfælde forvoldte IT-stop i timer*</b>	<b>480</b>	
<b>Antal tilfælde beskrevet:</b>		
Generende	92	
Alvorlige	36	
Katastrofale	3	

\*Af de der har angivet et præcist antal

## Bilag 2

# Omkring undersøgelsen

### **Kort om undersøgelsen**

Som nævnt i forordet indeholder denne redegørelse resultaterne fra den første fase i IT-Sikkerhedsrådets kortlægning af datasikkerheden i Danmark, omfattende perioden 1. januar 2000 til 31. december 2000.

Til brug for undersøgelsen har Danmarks Statistik udvalgt 1.200 virksomheder indenfor den offentlige og private sektor, som et repræsentativt udsnit af danske virksomheder og institutioner. Samtidig har IT- og Forskningsministeriet og IT-Sikkerhedsrådets medlemmer peget på ca. 400 virksomheder og institutioner som formodede "tungere" IT-anvendere til yderligere at indgå i undersøgelsen.

I alt ca. 1.600 virksomheder og institutioner har derefter modtaget en invitation om at deltage. Af disse meldte ca. 458 sig, hvoraf 441 har indsendt besvarelser. Dette er en svarprocent på ca. 27,6, hvilket må anses for et tilfredsstillende resultat for en 3-årig undersøgelse.

Besvarelserne er foretaget på 2 skemaer.

Det første skema "Staminformationer" udsendtes i november 2000 og omfatter virksomhedernes aktuelle beskyttelsesforanstaltninger.

Det andet skema "Hændelsesregistreringer" udsendtes medio januar 2001 og indeholder rapporteringer om de hændelser eller skader som de deltagende virksomheder har været udsat for i løbet af år 2000.

Skemaerne en vist sidst i rapporten.

## Virksomhedsfordeling - stamregistreringer

Fordelingen fremgår af nedenstående tabel.

Det skal bemærkes, at stamregistreringsskemaerne oprindeligt ikke indeholdt en kategorisering af uddannelsesinstitutioner og hospitaler og sygehuse. Da IT-Sikkerhedsrådet i forbindelse med bearbejdelsen af materialerne fandt, at dette ville være ønskeligt, rettedes henvendelse til IT- og Forskningsministeriet, der på grundlag af kendskabet til de deltagene virksomheders og institutioners navne, fremsendte en liste alene med numrene til analyseinstituttet, hvor disse numre efterfølgende kategoriseredes indenfor de nævnte områder.

Stamregistreringer	Antal	5<10	10<50	50<100	100<500	500<	I alt
Privat sektor	250	17	32	26	66	109	250
Offentlig sektor	191	7	15	29	66	74	191
<b>I alt</b>	<b>441</b>	<b>24</b>	<b>47</b>	<b>55</b>	<b>132</b>	<b>183</b>	<b>441</b>
<b>Branche:</b>							
Private:	250	17	32	26	66	109	<b>250</b>
Industri	70	2	2	5	19	42	70
Handel	52	4	10	7	17	14	52
Finans	26	3	3	1	6	13	26
Transport	11	0	2	2	1	6	11
Energi	6	0	0	1	1	4	6
Telekom	4	0	0	0	0	4	4
Byggeri	24	2	7	5	4	6	24
IT-service	14	1	1	0	5	7	14
Service	29	3	5	4	9	8	29
Andet	14	2	2	1	4	5	14
Offentlige	191	7	15	29	66	74	<b>191</b>
Adm. og forv.	87	1	3	5	40	38	87
Pleje og sundhed	5	2	0	0	2	1	5
Forsyning og transport	6	0	1	0	1	4	6
Servicefunkt.	12	1	2	4	2	3	12
Andet	27	3	3	3	9	9	27
Uddannelse	37	0	6	17	9	5	37
Hospital og Sygehuse	17	0	0	0	3	14	17
<b>I alt</b>	<b>441</b>	<b>24</b>	<b>47</b>	<b>55</b>	<b>132</b>	<b>183</b>	<b>441</b>

## Virksomhedsfordeling - hændelsesregistreringer

Svarfristen for indsendelse af hændelsesregistreringer var oprindeligt sat til den 15. februar 2001, men en stor del af deltagerne var forsinkede med deres besvarelse. Pr. 1. april var der indløbet 418 besvarelser, på hvilket grundlag tallene er opgjort.

Hændelsesregistreringer	Antal	5<10	10<50	50<100	100<500	500<	I alt
Privat sektor	232	16	30	26	61	99	232
Offentlig sektor	186	7	15	29	63	72	186
<b>I alt</b>	<b>418</b>	<b>23</b>	<b>45</b>	<b>55</b>	<b>124</b>	<b>171</b>	<b>418</b>
<b>Branche:</b>							
Private:	232	16	30	26	61	99	232
Industri	65	2	2	5	18	38	65
Handel	48	4	10	7	14	13	48
Finans	25	3	3	1	6	12	25
Transport	10	0	2	2	1	5	10
Energi	5	0	0	1	1	3	5
Telekom	3	0	0	0	0	3	3
Byggeri	23	2	6	5	4	6	23
IT-service	13	1	1	0	4	7	13
Service	27	2	4	4	9	8	27
Andet	13	2	2	1	4	4	13
Offentlige	186	7	15	29	63	72	186
Adm. og forv.	85	1	3	5	39	37	85
Pleje og sundhed	5	2	0	0	2	1	5
Forsyning og transport	6	0	1	0	1	4	6
Servicefunkt.	12	1	2	4	2	3	12
Andet	25	3	3	3	8	8	25
Uddannelse	36	0	6	17	8	5	36
Hospital og Sygehuse	17	0	0	0	3	14	17
<b>I alt</b>	<b>418</b>	<b>23</b>	<b>45</b>	<b>55</b>	<b>124</b>	<b>171</b>	<b>418</b>

Det skal bemærkes, at i hændelsesregistreringsskemaet er der - udover en angivelse af, hvorvidt deltagerens virksomhed/institution har været ramt af en hændelse på det pågældende område, også plads til angivelse af hvor mange tilfælde af hændelsen pågældende har været udsat for, samt en række andre underspecifikationer. Mange har udfyldt disse informationer med konkrete tal, andre har blot angivet "mange" eller et "?". Kun i det omfang der er angivet et konkret tal, er det medtaget i gennemsnitsangivelser.

På et enkelt område (spørgsmål 22 - Uautoriseret adgang) har nogle af besvarelsene været overordentlig specifikke, og der er angivet tal som eks. 7.237 i antal tilfælde. Det må antages at tallet er et udtryk for antal portscanninger, hvor andre har angivet antal forsøg. Tallene må derfor tages med et vist forbehold. Spørgsmålet præciseres nedre i næste runde.

På basis af de modtagne svar kan det konstateres, at nogle af deltagerne på enkelte områder, har haft vanskeligheder med at skelne mellem de ønskede oplysninger. Det drejer sig om spørgsmål 7 og 8 (henholdsvis "Telekommunikationsproblemer" og "Internetproblemer"), samt spørgsmål 11 og 18 (henholdsvis "Hændelige fejl og skader på IT-udstyr" og "HW-afbrud"). Spørgsmålene på disse områder vil blive nærmere præciseret i næste udsendelse af spørgeskemaerne.

**Bilag 3**

## Stamregistreringskema

*Forskningsministeriet*

## IT-SIKKERHEDSRÅDETS UNDERSØGELSER 2000-2003

---

### STAMINFORMATIONER

**SIDSTE AFLEVERINGSFRIST 1. DECEMBER 2000**

# IT-SIKKERHEDSRÅDETS UNDERSØGELSER 2000-2003

## STAMINFORMATIONER 1

### 1. Hvilken branche er Deres virksomhed primært tilknyttet (har den væsentligste omsætning indenfor)?

<input type="checkbox"/>	<b>Privat sektor:</b>	(Sæt kryds i den kategori der passer bedst hvis privat sektor)									
		Industri	<input type="checkbox"/>	Handel	<input type="checkbox"/>	Finans	<input type="checkbox"/>	Transport	<input type="checkbox"/>	Energi	<input type="checkbox"/>
		Telekom <small>(incl. ISP)</small>	<input type="checkbox"/>	Byggeri	<input type="checkbox"/>	IT-service <small>(incl. outsourcing-leverandører og servicebureauer)</small>	<input type="checkbox"/>	Service	<input type="checkbox"/>	Andet	<input type="checkbox"/>
<input type="checkbox"/>	<b>Offentlig sektor</b>	(Sæt kryds i den kategori der passer bedst hvis offentl. sektor)									
		offentl. adm. og forv.	<input type="checkbox"/>	offentl. pleje- og sundhed	<input type="checkbox"/>	offentl. forsyning og transport	<input type="checkbox"/>	offentl. servicefunkt.	<input type="checkbox"/>	offentl. andet	<input type="checkbox"/>

### 2. Hvor mange ansatte har virksomheden i Danmark?

Flere end 5 mindre end 10	<input type="checkbox"/>	Flere end 10 færre end 50	<input type="checkbox"/>	Flere end 50 færre end 100	<input type="checkbox"/>	Flere end 100 færre end 500	<input type="checkbox"/>	Flere end 500	<input type="checkbox"/>
---------------------------	--------------------------	---------------------------	--------------------------	----------------------------	--------------------------	-----------------------------	--------------------------	---------------	--------------------------

### 3. Har virksomheden selskaber/filialer/kontorer uden for Danmark?

Ja	<input type="checkbox"/>	Nej	<input type="checkbox"/>
----	--------------------------	-----	--------------------------

### 4. Drift af de vigtigste systemer varetages af:

Intern IT-afdeling eller firmaejet selskab hertil	<input type="checkbox"/>	Er Deres virksomhed outsourcing leverandør eller servicebureau - d.v.s. foretages IT-behandling for 3. part (eksterne kunder)	Ja <input type="checkbox"/> Nej <input type="checkbox"/>	Drift foretages hos outsourcing leverandør eller servicebureau	<input type="checkbox"/>	Foretages den primære drift på udstyr placeret udenfor Danmark	<input type="checkbox"/>
<i>Såfremt der svares ja til et eller begge ovenstående spørgsmål, bedes de efterfølgende spørgsmål besvaret for så vidt angår det personel, udstyr og/eller software, der alene er placeret på virksomhedens egne lokationer i Danmark</i>							

### 5. Hvor mange fuldtidsansatte er i IT-drifts-/produktionsafdelingen?

Ingen - funktionen er outsourcet	<input type="checkbox"/>	Ingen	<input type="checkbox"/>	Færre end 10	<input type="checkbox"/>	Flere end 10 færre end 50	<input type="checkbox"/>	Flere end 50 færre end 100	<input type="checkbox"/>	Flere	<input type="checkbox"/>
----------------------------------	--------------------------	-------	--------------------------	--------------	--------------------------	---------------------------	--------------------------	----------------------------	--------------------------	-------	--------------------------

### 6. Hvor mange fuldtidsansatte er i IT-systemudviklingsafdelingen?

Ingen - funktionen er outsourcet	<input type="checkbox"/>	Ingen	<input type="checkbox"/>	Færre end 10	<input type="checkbox"/>	Flere end 10 færre end 50	<input type="checkbox"/>	Flere end 50 færre end 100	<input type="checkbox"/>	Flere	<input type="checkbox"/>
----------------------------------	--------------------------	-------	--------------------------	--------------	--------------------------	---------------------------	--------------------------	----------------------------	--------------------------	-------	--------------------------

### 7. Hvor mange brugere er fast tilkøbt virksomhedens netværk?

Færre end 10	<input type="checkbox"/>	Flere end 10 færre end 100	<input type="checkbox"/>	Flere end 100 færre end 500	<input type="checkbox"/>	Flere end 500 færre end 1.000	<input type="checkbox"/>	Flere end 1.000	<input type="checkbox"/>
--------------	--------------------------	----------------------------	--------------------------	-----------------------------	--------------------------	-------------------------------	--------------------------	-----------------	--------------------------

### 8. Virksomhedens anvendelse af Internettet

<b>Egne ansattes brug</b>	Fri adgang til alle services	<input type="checkbox"/>	Skriftlige regler for brugen	<input type="checkbox"/>	Kun få services kan anvendes	<input type="checkbox"/>	Kun få eller ingen ansatte har adgang	<input type="checkbox"/>
---------------------------	------------------------------	--------------------------	------------------------------	--------------------------	------------------------------	--------------------------	---------------------------------------	--------------------------

<b>Virksomhedens tilstedeværelse på web</b>	Ingen	<input type="checkbox"/>	Alene til reklame	<input type="checkbox"/>	Reklame og kunderserv.	<input type="checkbox"/>	Reklame og ordremodt.	<input type="checkbox"/>	Reklame, ordremodt. og elektr. betaling	<input type="checkbox"/>
---	-------	--------------------------	-------------------	--------------------------	------------------------	--------------------------	-----------------------	--------------------------	---	--------------------------

# IT-SIKKERHEDSRÅDETS UNDERSØGELSER 2000-2003

## STAMINFORMATIONER 2

- Generel sikring 1

Spørgsmålene på dette skema har alene til formål at danne baggrund for undersøgelsen og må ikke tages som udtryk for, at spørgsmålene i deres helhed omfatter virksomhedens samlede sikkerhedsniveau.

### 9. Har virksomheden en beskrevet IT-sikkerhedspolitik godkendt af bestyrelse/direktion:

Nej

Ja  hvis ja:

Hvornår er den sidst ajourført (sæt kryds i relevant felt)?

Mere end 10 år siden

Mere end 5 år siden

Mere end 2 år siden

Mindre end 2 år siden

Sæt kun kryds i relevante felter, hvis ja

Indeholder den specificeret ansvar for datasikkerheden

Indeholder den en specifikation af, hvilke af virksomhedens områder, den dækker

Indeholder den konkrete mål for virksomhedens ønsker til datasikkerheden inden for de forskellige delområder

Er efterlevelse af IT-sikkerhedspolitikken gjort målbar

Fører virksomheden selv løbende kontrol med efterlevelsen - ud over en evt. årlig gennemgang af revisionen

### 10. Har virksomheden en formel IT-sikkerhedsorganisation?

Nej

Ja  hvis ja:

Sæt kun kryds i relevante felter, hvis ja:

Har virksomhedens et IT-sikkerhedsudvalg?

Har virksomheden en IT-sikkerhedschef/-leder/-koordinator?

Har virksomheden en intern revision, der beskæftiger sig med datasikkerheden?

Har virksomheden en ekstern revision, der beskæftiger sig med datasikkerheden?

# IT-SIKKERHEDSRÅDETS UNDERSØGELSER 2000-2003

## STAMINFORMATIONER 2

## - Generel sikring 2

11. Anvender virksomheden **formaliserede og dokumenterede** procedurer (eks. risiko-analyser) i forbindelse med større teknologi- og/eller systemændringer i virksomheden?

Ja

Nej

*hvis ja, sæt kun et kryds*

af og til

altid for bestemte områder

altid

12. Har virksomheden installeret aut. alarm-udstyr tilsluttet døgnbemandet alarmcentral (evt. egen) for følgende hændelser omkring kritisk IT-udstyr?

Ja

Nej

*hvis ja, sæt kun kryds i relevante felter*

Brand

Indbrud

Vandskade

13. Har virksomheden installeret følgende udstyr/systemer for de mest kritiske IT-områder?

Ja

Nej

*hvis ja, sæt kun kryds i relevante felter*

Adgangsbegrænsning

UPS

Nødstrømsgenerator

14. Har virksomheden indført fast registrering og/eller mærkning af alt udstyr (pc, modems, printere etc.) og software med henblik på forebyggelse, inventarfortegnelse og/eller efterlysning efter indbrud?

Ja

Nej

*sæt kun kryds hvis ja*

Fast registrering

Mærkning

15. Anvender virksomheden placering af backup af vitale data, programmer m.m. andetsteds end i den bygning, hvor det mest kritiske udstyr er placeret?

Ja

Nej



16. Har virksomheden en beredskabsplan for IT-funktionen til iværksættelse umiddelbart efter en hændelse, der lammer hele eller dele af IT-behandlingen over en længere periode (mere end 1 dag) ?

Ja

Nej

*hvis ja, sæt kun et kryds*

Indebærer at IT-funktionen genoptages i ønsket omfang inden for:

Under 2 dage  2 - 5 dage  5 - 10 dage  Mere end 10 dage

17. Hvis De har svaret ja til ovenstående spørgsmål oplys venligst, hvorvidt planen har været afstestet.

Ja

Nej

*hvis ja, sæt kun et kryds for hvert af de to nedenstående spørgsmål*

A. Kun delvis  eller i sin helhed

B. Testen er foretaget i år  sidste år  senere

18. Har virksomheden gennemført særlige sikringsforanstaltninger til sikring af sine telekommunikationsforbindelser?

Ja

Nej

*sæt kun kryds, hvis ja*

Teleforbindelser ad fysisk adskilte fremføringsveje

Teleforbindelser via flere centraler

Anvendes mere end en Internet Service Provider

19. Anvender virksomheden en eller flere firewalls til sikring mod udefra kommende transaktioner fra Internettet?

Ja

Nej

*sæt kun kryds, hvis ja*

Opdateres Deres Firewall opsætning løbende

Aftestes Deres Firewall opsætning regelmæssigt

20. Anvender virksomheden **digitale signaturer** på hele eller dele af sin kommunikation?

Ja

Nej

*hvis ja, sæt kun et kryds*

Frivilligt og kun i det omfang det er standard i systemet

Obligatorisk på al kritisk kommunikation

# IT-SIKKERHEDSRÅDETS UNDERSØGELSER 2000-2003

## STAMINFORMATIONER 2

## - Generel sikring 3

21. Anvender virksomheden kryptering på hele eller dele af sin kommunikation?

Ja   
Nej

*sæt kun kryds, hvis ja*

Frivilligt og kun i det omfang det er standard i systemet

Obligatorisk på al kritisk kommunikation

22. Abonnerer virksomheden på et eller flere anti-virus programmer?

Ja   
Nej

*sæt kun kryds, hvis ja*

Opdateres alle pc'er automatisk med de sidste nye opdateringer ved log-on

Omfatter abonnementet og opdateringen også hjemmearbejdsplads-pc'er

Omfatter abonnementet og opdateringen også hjemme-pc'er (under virksomhedsordningen) der ikke anvendes til arbejde for virksomheden

23. Anvender virksomheden et eller flere systemer til at opdage og registrere forsøg på at opnå uautoriseret adgang til systemer eller data - eks. et Internet Intrusion Detection System?

Ja   
Nej

*sæt kun kryds, hvis ja*

Kun på vitale systemer

På alle systemer

24. Anvender virksomheden en formaliseret procedure (Change Management), der fast anvendes eksempelvis ved overdragelse af nye/rettede programmer fra test til produktion?

Ja   
Nej

25. Har virksomheden en fast procedure for registrering af fejl og forsinkelser i produktionen?

Ja   
Nej

26. Har virksomheden gennemgået og eventuelt ændret eller tilrettelagt forretningsgange, således at virksomhedens IT-anvendelse helt efterlever kravene hertil i den nye datalovgivning?

Ja   
Nej

Det var det hele for denne gang.

Det der nu tilbagestår er, at De kontrollerer, at Deres firmanummer er påført forsiden af besvarelseskemaerne, forinden de sender besvarelseskemaet i den vedlagte kuvert (porto betalt) til PricewaterhouseCoopers, der står for den praktiske bearbejdning.

Såfremt Deres firmanummer ikke er påført forsiden af besvarelseskemaerne, bedes De selv påføre dette efter oplysning fra Forskningsministeriet.

De skal ikke underskrive bevarelserne eller påføre andre informationer end de felterne beder om.

Vi siger Dem tak for hjælpen.

IT-sikkerhedsrådet

**Bilag 4**

## Hændelseskema

## IT-SIKKERHEDSRÅDETS UNDERSØGELSER 2000-2003

Periode: 1.1.2000 - 31.12.2000

### Kære deltager i IT-sikkerhedsrådets undersøgelse

Indledningsvis vil jeg gerne udtrykke rådets taknemmelighed for Deres fortsatte støtte til IT-sikkerhedsrådets løbende undersøgelse omkring IT-sikkerheden i Danmark. Jeg kan oplyse, at der deltager ca. 450 virksomheder i undersøgelsen, hvilket er en svarprocent på ca. 28, og det mener vi er flot for en løbende 3-årig undersøgelse.

Det er vigtigt, at Deres besvarelser er så nøjagtige som muligt, for at undersøgelsens resultater kan anvendes. I denne første del af undersøgelsen ved vi, at De ikke har haft kendskab til spørgsmålene og følgelig ikke nødvendigvis har foretaget en løbende registrering af alle de områder der spørges om. Besvarelsen kan derfor tage lidt længere tid denne gang, end tilfældet vil være de efterfølgende gange.

### Perioden omfatter kun hændelser fra 1. januar 2000 til 31. december 2000

Vi beder Dem til brug for denne første del kun at besvare de aktuelle spørgsmål positivt, såfremt De er sikker på, at hændelserne har fundet sted i tidsrummet 1.1.2000 til 31.12.2000. *(Alle sikkerhedsmæssige hændelser før og efter dette tidsrum skal ikke medtages, da de blot vil forvrænge billedet).* Såfremt De ikke har registreret eller ikke kan erindre, hvor mange tilfælde af hændelsen, der har været i perioden, anfører de blot det antal, De er sikker på har forekommet (alternativt blot et). For at sige det kort - hellere underdrive end overdrive.

### Anonymiteten i højsædet

Husk kun at udfylde svarfelterne. De skal ikke kommentere, uddybe, underskrive, attestere eller lign. på blanketterne. Det skal understreges, at Forskningsministeriet alene kun kender navn og adresse på Deres virksomhed og det tilknyttede nummer og intet andet - og at analyseinstituttet kun kender de informationer, De indsender under det tilknyttede nummer. Ved således at holde informationerne totalt adskilt, kan De uden risiko afgive de ønskede informationer i fuld anonymitet - også selv om deres besvarelse skulle komme uvedkommende i hænde. Når De har udfyldt skemaet, bedes De kontrollere, at der er påsat en etiket på skemaets første side med Deres firmanummer. Det er den eneste identifikation af Dem som afsender. Uden dette nummer kan Deres besvarelse ikke anvendes. Hvis der ikke er etiket påsat med dette nummer, bedes De selv påføre nummeret (dette kan De evt. få oplyst fra Forskningsministeriet, ifald de måtte have glemt det). Besvarelsen lægges derefter i den forudfrankererede kuvert og postes. Vi har overvejet at lave skemaerne på Internettet, men der vil vi ikke med sikkerhed kunne beskytte Deres anonymitet.

### Næste hændelsesskema - til Deres orientering

Det næste hændelsesregistreringsskema vil omfatte første halvår af 2001 og påregnes udsendt medio juli 2001. Vi forventer, at spørgsmålene stort set vil omfatte de samme områder som i denne første del. Det er for at kunne følge udviklingen i skadesbilledet (naturligvis med respekt for evt. nye risici, der måtte fremkomme i mellemtiden og erfaringerne fra de første spørgeskemaer). P.t. overvejer vi, hvorvidt det kunne være hensigtsmæssigt også at få angivet nogle beløbsmæssige størrelser for evt. in- og eksterne omkostninger (til eks. konsulenthjælp, teknikker, reparationer etc.) til udbedring af de skader, som hændelsen har medført

IT-sikkerhedsrådet vil sætte stor pris på, at De - i det omfang De ikke allerede måtte have løbende registrering af disse informationer - vil overveje at indføre sådanne snarest belejligt. Det er nøgleinformationer til Deres beslutninger ved opretholdelsen af den vanskelige balance mellem risici, sikkerhed og økonomi, og en effektiv rapportering af indtrufne skader vil gavne hele Danmarks effektive udnyttelse af IT-teknologien.

På forhånd tak for Deres velvillige bistand.

Mads Bryde Andersen  
Formand for IT-sikkerhedsrådet

## IT-SIKKERHEDSRÅDETS UNDERSØGELSER 2000-2003

Periode: 1.1.2000 - 31.12.2000

### Kære deltager i IT-sikkerhedsrådets undersøgelse

Indledningsvis vil jeg gerne udtrykke rådets taknemmelighed for Deres fortsatte støtte til IT-sikkerhedsrådets løbende undersøgelse omkring IT-sikkerheden i Danmark. Jeg kan oplyse, at der deltager ca. 450 virksomheder i undersøgelsen, hvilket er en svarprocent på ca. 28, og det mener vi er flot for en løbende 3-årig undersøgelse.

Det er vigtigt, at Deres besvarelser er så nøjagtige som muligt, for at undersøgelsens resultater kan anvendes. I denne første del af undersøgelsen ved vi, at De ikke har haft kendskab til spørgsmålene og følgelig ikke nødvendigvis har foretaget en løbende registrering af alle de områder der spørges om. Besvarelsen kan derfor tage lidt længere tid denne gang, end tilfældet vil være de efterfølgende gange.

### Perioden omfatter kun hændelser fra 1. januar 2000 til 31. december 2000

Vi beder Dem til brug for denne første del kun at besvare de aktuelle spørgsmål positivt, såfremt De er sikker på, at hændelserne har fundet sted i tidsrummet 1.1.2000 til 31.12.2000. *(Alle sikkerhedsmæssige hændelser før og efter dette tidsrum skal ikke medtages, da de blot vil forvrænge billedet).* Såfremt De ikke har registreret eller ikke kan erindre, hvor mange tilfælde af hændelsen, der har været i perioden, anfører de blot det antal, De er sikker på har forekommet (alternativt blot et). For at sige det kort - hellere underdrive end overdrive.

### Anonymiteten i højsædet

Husk kun at udfylde svarfelterne. De skal ikke kommentere, uddybe, underskrive, attestere eller lign. på blanketterne. Det skal understreges, at Forskningsministeriet alene kun kender navn og adresse på Deres virksomhed og det tilknyttede nummer og intet andet - og at analyseinstituttet kun kender de informationer, De indsender under det tilknyttede nummer. Ved således at holde informationerne totalt adskilt, kan De uden risiko afgive de ønskede informationer i fuld anonymitet - også selv om deres besvarelse skulle komme uvedkommende i hænde. Når De har udfyldt skemaet, bedes De kontrollere, at der er påsat en etiket på skemaets første side med Deres firmanummer. Det er den eneste identifikation af Dem som afsender. Uden dette nummer kan Deres besvarelse ikke anvendes. Hvis der ikke er etiket påsat med dette nummer, bedes De selv påføre nummeret (dette kan De evt. få oplyst fra Forskningsministeriet, ifald de måtte have glemt det). Besvarelsen lægges derefter i den forudfrankererede kuvert og postes. Vi har overvejet at lave skemaerne på Internettet, men der vil vi ikke med sikkerhed kunne beskytte Deres anonymitet.

### Næste hændelsesskema - til Deres orientering

Det næste hændelsesregistreringsskema vil omfatte første halvår af 2001 og påregnes udsendt medio juli 2001. Vi forventer, at spørgsmålene stort set vil omfatte de samme områder som i denne første del. Det er for at kunne følge udviklingen i skadesbilledet (naturligvis med respekt for evt. nye risici, der måtte fremkomme i mellemtiden og erfaringerne fra de første spørgeskemaer). P.t. overvejer vi, hvorvidt det kunne være hensigtsmæssigt også at få angivet nogle beløbsmæssige størrelser for evt. in- og eksterne omkostninger (til eks. konsulenthjælp, teknikker, reparationer etc.) til udbedring af de skader, som hændelsen har medført

IT-sikkerhedsrådet vil sætte stor pris på, at De - i det omfang De ikke allerede måtte have løbende registrering af disse informationer - vil overveje at indføre sådanne snarest belejligt. Det er nøgleinformationer til Deres beslutninger ved opretholdelsen af den vanskelige balance mellem risici, sikkerhed og økonomi, og en effektiv rapportering af indtrufne skader vil gavne hele Danmarks effektive udnyttelse af IT-teknologien.

På forhånd tak for Deres velvillige bistand.

Mads Bryde Andersen  
Formand for IT-sikkerhedsrådet

### LÆS VENLIGST DENNE BESKRIVELSE INDEN DE UDFYLDER SKEMAET.

Spørgeskemaerne indeholder 24 spørgsmål vedrørende udvalgte områder af relevans for datasikkerheden. For at sikre den bedst mulige forståelse af det enkelte spørgsmål, er de alle opbygget over den samme ramme som forklaret nedenfor.

Her er emneområdet angivet

Her er hovedspørgsmålet formuleret

Spørgsmålene besvares ved afkrydsning af Ja/Nej kasserne. I få tilfælde (spørgsmål 21-24) kan der angives svaret VED IKKE.

Hvis svaret er Ja udfyldes det grå felt med specifikationer.

**STRØMPROBLEMER**

5. Har virksomheden i den forløbne periode haft problemer med strømforsyningen i form af eks. strømsvingninger, lynnedslag, strøm-afbrydelser eller lign., der har medført problemer for IT-produktionen?

Ja

Nej

*hvis ja*

Angiv antal tilfælde

*kun kryds i relevante felter for ja:*

Strømsvingninger der påvirkede IT-produktionen

Strømafbrydelser

Lynnedslag, der påvirkede IT-produktionen

Værste tilfælde forvoldte IT-stop i timer

I det værste tilfælde var konsekvenserne for virksomheden (kun et kryds):

Generende  Alvorlig  Katastrofal

*Her kan der være forklarende undertekster til spørgsmålet.*

Hvor teksten er angivet med **fed (bold)** beder vi Dem venligst svare med et så nøjagtigt antal (uden decimaler) som muligt.

Næsten alle spørgsmål har et eller flere af sådanne. Som hovedregel vil det ene af disse være et spørgsmål om, hvor mange tilfælde der har været i perioden.

Det andet spørgsmål vil (medmindre andet er angivet) være antallet af timer (eller anden angivet enhed) det pågældende problem har forvoldt produktionsstop eller alvorligere driftsmæssige problemer/forsinkelser. Udtrykket IT-stop dækker således over såvel et total IT-stop som et afbrud eller alvorlige produktionsproblemer på berørt software.

Har hændelse(erne) ikke medført produktionsstop eller alvorligere forsinkelser anføres blot et 0 i feltet.

Alle spørgsmål afsluttes med en vurdering af skadens betydning for den besvarende virksomhed.

Der bør angives effekten af skaden på virksomheden og ikke på den pågældende funktion/applikation der er blevet berørt af skaden.

**Bemærk venligst**, at selvom skaden eventuelt ikke har medført produktionsstop eller alvorligere forsinkelser, kan konsekvensen for virksomheden godt have været såvel generende, alvorlig som katastrofal.

# IT-SIKKERHEDSRÅDETS UNDERSØGELSER 2000-2003

## BESVARELSER 1

Periode: 1.1.2000 - 31.12.2000

**Registreringen omfatter kun hændelser indtruffet mellem 1. januar 2000 og 31. december 2000**

### BRAND

1. Har virksomheden i den forløbne periode været udsat for en eller flere brande?

Ja   
Nej

Bemærk venligst:

Følgeskader på data, udstyr og lokaler, som eks. skader der opstår som følge af slukningen, efterfølgende korrosion m.v. tæller i denne forbindelse også som brandskader.

hvis ja

Angiv antal tilfælde

\_\_\_\_\_ kun kryds i relevante felter for ja:

Ødelagdes data i forbindelse med brand

Blev IT-udstyr skadet af brand

Blev lokaler med IT-udstyr skadet af brand

Værste tilfælde forvoldte IT-stop i timer

I det værste tilfælde var konsekvenserne for virksomheden (kun et kryds):

Generende  Alvorlig  Katastrofal

### INDBRUD

2. Har virksomheden i den forløbne periode haft et eller flere indbrudsforsøg?

Ja   
Nej

Se nedenunder for vedr. "tyveri uden synlige tegn på indbrud".

hvis ja

Angiv antal tilfælde

\_\_\_\_\_ kun kryds i relevante felter for ja:

Blev der stjålet IT-udstyr

Blev der stjålet data (udover de i IT-udstyret indeholdte)

Blev der begået hærværk på andet IT-udstyr og/eller data

Værste tilfælde forvoldte IT-stop i timer

I det værste tilfælde var konsekvenserne for virksomheden (kun et kryds):

Generende  Alvorlig  Katastrofal

### TYVERI

3. Har virksomheden i den forløbne periode været udsat for tyveri af IT-udstyr og/eller data - uden synlige tegn, der tyder på indbrudstyveri?

Ja   
Nej

hvis ja

Angiv antal tilfælde

\_\_\_\_\_ kun kryds i relevante felter for ja:

Blev der stjålet IT-udstyr

Blev der stjålet data (udover de i IT-udstyret indeholdte)

Værste tilfælde forvoldte IT-stop i timer

I det værste tilfælde var konsekvenserne for virksomheden (kun et kryds):

Generende  Alvorlig  Katastrofal

### VANDSKADE

4. Har virksomheden i den forløbne periode været udsat for vandskader?

Ja   
Nej

hvis ja

Angiv antal tilfælde

\_\_\_\_\_ kun kryds i relevante felter for ja:

Kom vandet udefra (utæt tag, oversvømmede kloaker, stormflod etc.)

Kom vandet indefra (rørbrud, sprinkler, køl, etc.)

Værste tilfælde forvoldte IT-stop i timer

I det værste tilfælde var konsekvenserne for virksomheden (kun et kryds):

Generende  Alvorlig  Katastrofal

# IT-SIKKERHEDSRÅDETS UNDERSØGELSER 2000-2003

## BESVARELSER 2

Periode: 1.1.2000 - 31.12.2000

### Registreringen omfatter kun hændelser indtruffet mellem 1. januar 2000 og 31. december 2000

#### STRØMPROBLEMER

5. Har virksomheden i den forløbne periode haft problemer med strømforsyningen i form af eks. strømsvingninger, lynnedslag, strømafbrydelser eller lign., der har medført problemer for IT-produktionen?

Ja   
Nej

hvis ja

Angiv antal tilfælde

\_\_\_\_\_ kun kryds i relevante felter for ja:

Strømsvingninger der påvirkede IT-produktionen

Strømafbrydelser

Lynnedslag, der påvirkede IT-produktionen

Værste tilfælde forvoldte IT-stop i timer

I det værste tilfælde var konsekvenserne for virksomheden (kun et kryds):

Generende  Alvorlig  Katastrofal

#### ANDRE FORSYNINGSPROBLEMER

6. Har virksomheden i den forløbne periode haft andre problemer omkring forsyninger der kan påvirke IT-produktionen - eks. vand og køl?

Ja   
Nej

hvis ja

Angiv antal tilfælde

Værste tilfælde forvoldte IT-stop i timer

I det værste tilfælde var konsekvenserne for virksomheden (kun et kryds):

Generende  Alvorlig  Katastrofal

#### TELEKOMMUNIKATIONSPROBLEMER

7. Har virksomheden i den forløbne periode haft problemer med telekommunikationslinierne, der anvendes til IT-produktionen, herunder virksomhedens internetforbindelser?

Ja   
Nej

hvis ja

Angiv antal tilfælde

\_\_\_\_\_ kun kryds i relevante felter for ja:

Fejl og forsinkelser på transmissionen

Leveringsproblemer med nye og/eller ændringer

Afbrydelser af forbindelse

Værste tilfælde forvoldte IT-stop i timer

I det værste tilfælde var konsekvenserne for virksomheden (kun et kryds):

Generende  Alvorlig  Katastrofal

#### INTERNETPROBLEMER

8. Har virksomheden i den forløbne periode haft problemer med adgangen til/fra Internettet.

Ja   
Nej

hvis ja

Angiv antal tilfælde

\_\_\_\_\_ kun kryds i relevante felter for ja:

Fejl i egne internetapplikationer

Fejl eller nedbrud hos Internetleverandøren

Mangl. tilgængelighed hos samarb. partnere eller leverandører (udover internetleverandører)

Værste tilfælde forvoldte IT-stop i timer

I det værste tilfælde var konsekvenserne for virksomheden (kun et kryds):

Generende  Alvorlig  Katastrofal

# IT-SIKKERHEDSRÅDETS UNDERSØGELSER 2000-2003

## BESVARELSER 3

Periode: 1.1.2000 - 31.12.2000

Registreringen omfatter kun hændelser indtruffet mellem 1. januar 2000 og 31. december 2000

### SABOTAGE

9. Har virksomheden i den forløbne periode været udsat for fysiske sabotageforsøg, hærværk eller trusler mod de fysiske IT-installationer eller lign.?

Ja   
Nej

hvis ja

Angiv antal tilfælde

\_\_\_\_\_ kun kryds i relevante felter for ja:

Fysiske sabotageforsøg

Hærværk

Trusler der tages alvorligt

Værste tilfælde forvoldte IT-stop i timer

I det værste tilfælde var konsekvenserne for virksomheden (kun et kryds):

Generende  Alvorlig  Katastrofal

### ARBEJDSNEDLÆGGELSER OG STREJKER

10. Har virksomheden i den forløbne periode været ramt af arbejdsnedlæggelser, strejke eller anden afbrydelse af arbejdet forårsaget af virksomhedens IT-medarbejdere?

Ja   
Nej

hvis ja

Angiv antal tilfælde

\_\_\_\_\_ kun kryds i relevante felter for ja:

Massive sygemeldinger

Ulovlige arbejdsnedlæggelser

Strejker

Værste tilfælde forvoldte IT-stop i timer

I det værste tilfælde var konsekvenserne for virksomheden (kun et kryds):

Generende  Alvorlig  Katastrofal

### HÆNDELIGE FEJL OG SKADER PÅ IT-UDSTYR

11. Har virksomheden i den forløbne periode været ramt af hændelige fysiske skader og fysiske fejl på IT-udstyr, der har medført IT-stop?

Ja   
Nej

hvis ja

Angiv antal tilfælde

\_\_\_\_\_ kun kryds i relevante felter for ja:

Computere (servere, main-frames etc.)

Netværk (kabler, krydsfelter etc.)

Egne forsyningsenheder (transformatorer, køleudstyr etc.)

Værste tilfælde forvoldte IT-stop i timer

I det værste tilfælde var konsekvenserne for virksomheden (kun et kryds):

Generende  Alvorlig  Katastrofal

### ANDRE OMRÅDER

12. Har virksomheden i den forløbne periode været udsat for klager fra medarbejdere, tillidsrepræsentanter, fagforeninger eller andre, vedrørende virksomhedens anvendelse af TV-overvågning, registrering af internetanvendelse eller registrering af e-mails?

Ja   
Nej

hvis ja

Angiv antal tilfælde

Angiv venligst af hvilke årsag(er) - kun kryds for ja: \_\_\_\_\_

TV-overvågning

Internetanvendelse

Ind- og udgående e-mails

I det værste tilfælde var konsekvenserne for virksomheden (kun et kryds):

Generende  Alvorlig  Katastrofal

# IT-SIKKERHEDSRÅDETS UNDERSØGELSER 2000-2003

## BESVARELSER 4

Periode: 1.1.2000 - 31.12.2000

Registreringen omfatter kun hændelser indtruffet mellem 1. januar 2000 og 31. december 2000

### IT-MISBRUG

13. Har virksomheden i den forløbne periode været udsat for IT-misbrug af økonomisk karakter?

Ja   
Nej

**UAUTORISERET SALG:**  
Eks. salg af "kasseret" udstyr - eller udstyr bevidst forkert mærket "kasseret" - solgt til uvedkommende.  
**IT-BEDRAGERI**  
Uautoriseret overførsel af penge fra firmaet, dets kunder eller medarbejdere til uvedkommende. Dobbelt fakturering og lign.  
**MANIPULATION AF DATA**  
Uautoriseret ændring af data. Eks. ændring af salgspris for billigere køb til egen eller venners vinding, ændring af nøgleparametre for at skade beslutningsprocessen eller lign.  
**SLETNING AF DATA**  
Uautoriseret bevidst sletning af data og eller programmer

hvis ja

Angiv antal tilfælde

\_\_\_\_\_ kun kryds i relevante felter for ja:

	Mistanke	Bevis	Mistanke om interne involv.
Uautoriseret salg	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
IT-bedrageri	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Manipulation af data	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Bevidst sletning af data	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Andet	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

I det værste tilfælde var konsekvenserne for virksomheden (kun et kryds):

Generende  Alvorlig  Katastrofal

### INDUSTRISPIONAGE

14. Har virksomheden i den forløbne periode haft mistanke om eller været udsat for industrispionage eller bevidst afsløring af informationer til uvedkommende?

Ja   
Nej

hvis ja

Angiv antal tilfælde

\_\_\_\_\_ kun kryds i relevante felter for ja:

	Mistanke	Bevis
Industrispionage fra fremmede nationer	<input type="checkbox"/>	<input type="checkbox"/>
Industrispionage fra konkurrenter	<input type="checkbox"/>	<input type="checkbox"/>
Industrispionage fra andre	<input type="checkbox"/>	<input type="checkbox"/>
Bevidst afsløring af data	<input type="checkbox"/>	<input type="checkbox"/>

I det værste tilfælde var konsekvenserne for virksomheden (kun et kryds):

Generende  Alvorlig  Katastrofal

### TRUSLER MOD DATA ELLER SOFTWARE

15. Har virksomheden i den forløbne periode været udsat for afpresning ved hjælp af trusler rettet mod virksomhedens data eller software?

Ja   
Nej

Det kan eks. være i forbindelse med trusler om udløsning af eller manglende demontering af "trojanske heste", hemmeligt placeret et eller flere steder i virksomhedens IT-systemer eller anden software.

Et andet eksempel kunne være at kryptografer virksomhedens vitale databaser eller programbiblioteker, og forlange penge eller andre aktiver for udlevering af nøglen hertil.

hvis ja

Angiv antal tilfælde

\_\_\_\_\_ kun kryds i relevante felter for ja:

Er truslerne blevet effektueret?   
Er truslerne stadig aktive?

I det værste tilfælde var konsekvenserne for virksomheden (kun et kryds):

Generende  Alvorlig  Katastrofal

### OPHAVSRET M.M.

16. Har virksomheden i den forløbne periode været sigtet, anklaget eller været genstand for søgsmål vedrørende ophavsret, markedsføring, straffelovens bestemmelser vedr. IT-kriminalitet, mønsterbeskyttelse (relateret til IT-anvendelsen), patentkrænkelser eller har virksomheden anmeldt/rejst sag mod andre desangående?

Ja   
Nej

hvis ja

Angiv antal tilfælde

\_\_\_\_\_ kun kryds i relevante felter for ja:

Virksomheden sigtet for/ sagsøgt:		Virksomheden har anmeldt/rejst sag mod andre:
<input type="checkbox"/>	Ophavsret	<input type="checkbox"/>
<input type="checkbox"/>	Markedsføringsloven	<input type="checkbox"/>
<input type="checkbox"/>	Straffeloven	<input type="checkbox"/>
<input type="checkbox"/>	Mønsterbeskyttelse	<input type="checkbox"/>
<input type="checkbox"/>	Patentloven	<input type="checkbox"/>

I det værste tilfælde var konsekvenserne for virksomheden (kun et kryds):

Generende  Alvorlig  Katastrofal

# IT-SIKKERHEDSRÅDETS UNDERSØGELSER 2000-2003

## BESVARELSER 5

Periode: 1.1.2000 - 31.12.2000

Registreringen omfatter kun hændelser indtruffet mellem 1. januar 2000 og 31. december 2000

### BACKUP

17. Har virksomheden i den forløbne periode haft problemer med anvendelsen af backup af data og/eller programmer?

Ja

Nej

Som eksempler herpå kan bl.a. nævnes:

- for gammel backup
- utilstrækkelig backup
- mangl. backup (ikke taget)
- forsvundet backup
- ulæsbar backup
- utilgængelig backup

hvis ja

Angiv antal tilfælde

Angiv venligst: \_\_\_\_\_

Værste tilfælde forvoldte IT-stop i timer

I det værste tilfælde var konsekvenserne for virksomheden (kun et kryds):

Generende  Alvorlig  Katastrofal

### HW-AFBRUD

18. Har virksomheden i den forløbne periode haft betydelige afbrud i IT-produktionen som følge af fejl i IT-udstyr (hardwaren)?

Ja

Nej

hvis ja

Angiv antal tilfælde

Angiv venligst: \_\_\_\_\_

Værste tilfælde forvoldte IT-stop i timer

I det værste tilfælde var konsekvenserne for virksomheden (kun et kryds):

Generende  Alvorlig  Katastrofal

### SOFTWAREFEJL

19. Har virksomheden i den forløbne periode haft betydelige afbrud eller væsentlige fejl i IT-produktionen som følge af softwareproblemer?

Ja

Nej

hvis ja

Angiv antal tilfælde

\_\_\_\_\_ kun kryds i relevante felter for ja:

Styresystem

Standardapplikationer (indkøbte/lejede/leasede)

Egne udviklede applikationer

Værste tilfælde forvoldte IT-stop i timer

I det værste tilfælde var konsekvenserne for virksomheden (kun et kryds):

Generende  Alvorlig  Katastrofal

### IT-MEDARBEJDERAFGANG

20. Har virksomheden i den forløbne periode mistet IT-medarbejdere i et efter virksomhedens opfattelse for stort antal?

Ja

Nej

hvis ja

Angiv venligst ca. procentdel af IT-medarbejderne, der har forladt virksomheden i perioden:

>10<15%  >15<20%  >20<25%  Mere

I det værste tilfælde var konsekvenserne for virksomheden (kun et kryds):

Generende  Alvorlig  Katastrofal

# IT-SIKKERHEDSRÅDETS UNDERSØGELSER 2000-2003

## BESVARELSER 6

Periode: 1.1.2000 - 31.12.2000

### Registreringen omfatter kun hændelser indtruffet mellem 1. januar 2000 og 31. december 2000

#### VIRUS ANGREB

21. Er virksomheden i den forløbne periode blevet angrebet og inficeret af pc-virus, orme, trojanske heste m.m.?

Ja   
Nej   
Ved ikke

hvis ja

Angiv antal tilfælde

Angiv venligst: \_\_\_\_\_

I perioden er der samlet anvendt tid til bekæmpelse og opretning af alle virus-skader på ialt ca. person dage:

I det værste tilfælde anvendtes til opretning ca. person dage:

I det værste tilfælde havde vi driftsproblemer i kalenderdage

I det værste tilfælde var konsekvenserne for virksomheden (kun et kryds):

Generende  Alvorlig  Katastrofal

#### UAUTORISERET ADGANG

22. Har virksomheden i den forløbne periode været udsat for forsøg på at opnå uautoriseret adgang til systemer eller data via Internettet?

Ja   
Nej   
Ved ikke

hvis ja

Angiv antal tilfælde

\_\_\_\_\_ kun kryds i relevante felter for ja:

Antal tilfælde det opdagedes og afvist inden indtrængning

Antal vellykkede tilfælde

I det værste tilfælde anvendtes person dage til efterforskning og udbedring

I det værste tilfælde var konsekvenserne for virksomheden (kun et kryds):

Generende  Alvorlig  Katastrofal

#### DENIAL OF SERVICE

23. Har virksomheden i den forløbne periode været udsat for ude-af-drift angreb (denial-of-service attacks)?

Ja   
Nej   
Ved ikke

hvis ja

Angiv antal tilfælde

Angiv venligst: \_\_\_\_\_

Det værste angreb strakte sig over (timer)

I det værste tilfælde var konsekvenserne for virksomheden (kun et kryds):

Generende  Alvorlig  Katastrofal

#### E-MAIL

24. Har virksomheden i den forløbne periode været udsat for problemer med virksomhedens e-mail systemer, der har medført tab af e-mails eller større forsinkelser og/eller driftsstop?

Ja   
Nej   
Ved ikke

hvis ja

Angiv antal tilfælde

\_\_\_\_\_ kun kryds i relevante felter for ja:

Større forsinkelser

Tab af mails i ukendt/større antal

Driftsstop

Værste tilfælde forvoldte IT-stop i timer

I det værste tilfælde var konsekvenserne for virksomheden (kun et kryds):

Generende  Alvorlig  Katastrofal