Monitor
Deloitte.

IT-sikkerhed og datahåndtering i danske SMV'er

Monitor Deloitte for Erhvervsstyrelsen

April 2018

Indhold

1 Ledelsesresume

Danmark er et af de mest digitaliserede lande i Europa, men IT-sikkerheden i danske virksomheder er ikke fulgt med den høje digitaliseringsgrad. Indeværende undersøgelse viser, at mange virksomheder har haft brud på IT-sikkerheden, og at endnu flere er i risikozonen. 39 procent af de små og mellemstore virksomheder (SMV'er) har et IT-sikkerhedsniveau, der vurderes utilstrækkeligt i forhold til deres risikoprofil. SMV'erne oplever blandt andet, at barriererne for at øge IT-sikkerheden er medarbejdernes manglende imødekommenhed overfor forandringer og ledelsens manglende engagement i IT-sikkerhed.

Monitor Deloitte har for Erhvervsstyrelsen udarbejdet et statusbillede af IT-sikkerhedsniveauet i danske SMV'er. Dette er sket med henblik på at kortlægge, om danske SMV'er har et tilstrækkeligt IT-sikkerhedsniveau, og om de har tilpasset deres indsats på området, efterhånden som IT-kriminalitet er steget i omfang.

Ifølge Europa-Kommissionens indeks for den digitale økonomi og det digitale samfund (DESI) fra 2017 er Danmark det land i EU, der har den mest digitaliserede økonomi, og det skaber muligheder for innovation og vækst. Den øgede afhængighed af IT øger dog samtidig risikoen for forskellige former for IT-sikkerhedsangreb fra hackere og andre IT-kriminelle. Disse angreb dækker for eksempel over phishingmails, der kan inficere en virksomheds systemer med ransomware, eller angreb fra hackere, der udnytter sårbarheder i en virksomheds IT-systemer. Dansk erhvervsliv har de seneste år stået overfor et stigende trusselsbillede, og i februar 2017 vurderede Center for Cybersikkerhed (CFCS), at truslen mod Danmark er høj. Det gælder i særlig grad IT-spionage og IT-kriminalitet rettet mod både myndigheder, virksomheder og privatpersoner. CFCS nævner desuden, at der igennem de seneste år har været en stigning i antallet af IT-sikkerhedsangreb og dermed forsøg på at kompromittere danske virksomheder og myndigheder.[1] Det kan have store konsekvenser for virksomhederne.

Denne undersøgelse viser, at 14 procent har haft et IT-sikkerhedsbrud, men tallet kan være højere
På baggrund af svar fra mere end 1.000 virksomheder viser estimatet i indeværende undersøgelse, at cirka 14 procent af SMV'erne har oplevet et brud på deres IT-sikkerhed. Det svarer til cirka 11.000 virksomheder. Heraf har 43 procent haft et IT-sikkerhedsbrud indenfor det seneste år, svarende til 4.700 SMV'er. Tallets nøjagtighed er dog forbundet med en høj grad af usikkerhed. Mange virksomheder er tilbageholdende med at dele, hvis de har lidt et IT-sikkerhedsbrud, hvilket blandt andet understreges af, at 28 procent af virksomhederne har kendskab til, at en samarbejdspartner har haft et IT-sikkerhedsbrud. Der kan desuden også være virksomheder, der ikke har opdaget, at de har haft et IT-sikkerhedsbrud, for eksempel hvis der har været tale om erhvervsspionage, hvor gerningsmanden har forsøgt at slippe uset ind. Mørketal som disse kan indebære, at undersøgelsen underestimerer problemets egentlige omfang.

39 procent af danske SMV'er har ikke et tilstrækkeligt IT-sikkerhedsniveau
Undersøgelsen tyder samtidig på, at mange SMV'ers IT-sikkerhedsniveau ikke er tilstrækkelig højt set i forhold til virksomhedernes risikoprofil. Med andre ord synes de tiltag og foranstaltninger, virksomhederne har gjort for at sikre deres IT-sikkerhed, utilstrækkelige set i forhold til virksomhedernes afhængighed af systemer og følsomme data. Dette fremgår af tabel 1, hvor virksomhedernes IT-sikkerhedsniveau holdes sammen med virksomhedernes risikoprofil.

[1] https://fe-ddis.dk/cfcs/CFCSDocuments/Cybertruslen%20mod%20Danmark.pdf

Tabel 1. SMV'ers vægtede fordeling indenfor arketyperne, det vil sige sammenhæng mellem virksomhedernes IT-sikkerhedsniveau og risikoprofil

		IT-sikkerhedsniveau		
		Lavt	Middel	Højt
Risikoprofil	Høj	**De sårbare:** 39 procent		
	Middel		**De tilpas sikrede:** 46 procent	
	Lav			**De påpasselige:** 15 procent

Kilde: Wilke for Monitor Deloitte og Monitor Deloitte-analyse

De grå felter i Tabel 1 er et udtryk for de virksomheder, hvor IT-sikkerhedsniveauet fremstår utilstrækkeligt i forhold til deres risikoprofil, det vil sige en kombination af, hvor alvorligt et IT-sikkerhedsbrud vil være for virksomheden, og hvor stor sandsynligheden er for, at virksomheden bliver ramt. 39 procent af virksomhederne placerer sig i denne kategori, og dermed anslås de at være mere sårbare overfor eventuelle IT-sikkerhedsangreb.

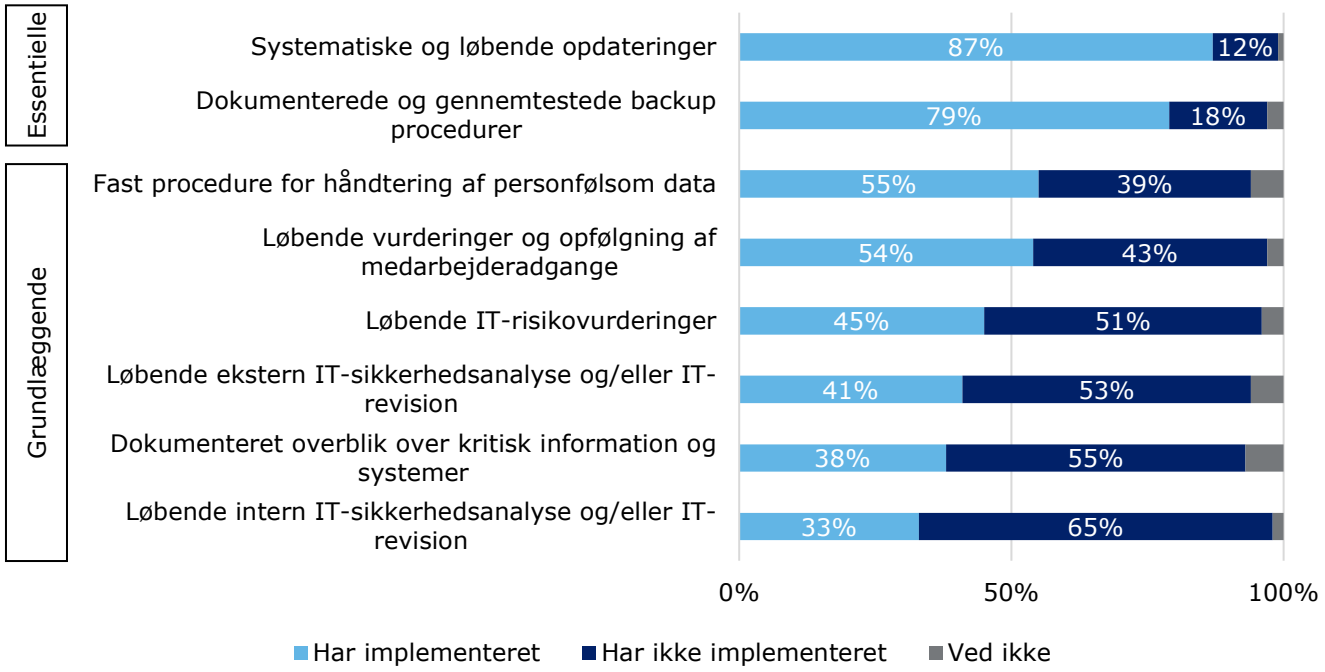
De påpasselige SMV'er er virksomheder, der har et sikkerhedsniveau, der er højere end deres risikoprofil. Virksomhederne er karakteriseret ved en lav eller middel grad af afhængighed af systemer og følsomme data. Omvendt har alle virksomhederne sikret grundlæggende foranstaltninger og flere avancerede tiltag. **De tilpas sikre SMV'er** er virksomheder, der har et IT-sikkerhedsniveau, der er tilpasset deres risikoprofil. **De sårbare SMV'er** er virksomheder, der har et IT-sikkerhedsniveau, der er lavere, end deres risikoprofil tilsiger. Det er typisk virksomheder, der er afhængige af systemer i den daglige drift og af en eller flere typer følsomme data.

Det er vigtigt at være opmærksom på, at selv hvis man som virksomhed har tilpasset sit IT-sikkerhedsniveau til sin risikoprofil eller endda har et højere IT-sikkerhedsniveau, end ens risikoprofil tilsiger, kan man alligevel godt blive ramt af et IT-sikkerhedsbrud, og et højt IT-sikkerhedsniveau er ingen garanti for, at man undgår et IT-sikkerhedsbrud. Dette betyder dog ikke, at virksomhederne ikke skal investere i IT-sikkerhed, da god IT-sikkerhed kan reducere sårbarheden overfor IT-sikkerhedsbrud og være et godt middel til risikostyring.

Knap en fjerdedel af SMV'erne har ikke implementeret essentielle IT-sikkerhedsforanstaltninger

88 procent af de danske SMV'er har implementeret systematiske og løbende opdateringer, mens 82 procent har dokumenterede og gennemtestede backupprocedurer, som det fremgår Figur 1. Disse to IT-sikkerhedsforanstaltninger anses som værende helt essentielle for en virksomheds IT-sikkerhed. Ser man på de to faktorer samlet, er der dog en stor del, der ikke har implementeret begge IT-sikkerhedsforanstaltninger. 23 procent af de danske SMV'er, svarende til knap en fjerdedel, har ikke implementeret begge disse essentielle IT-sikkerhedsforanstaltninger som en del af deres IT-sikkerhed.

Figur 1. Andel af danske SMV'er, der har implementeret essentielle og grundlæggende IT-sikkerhedsforanstaltninger



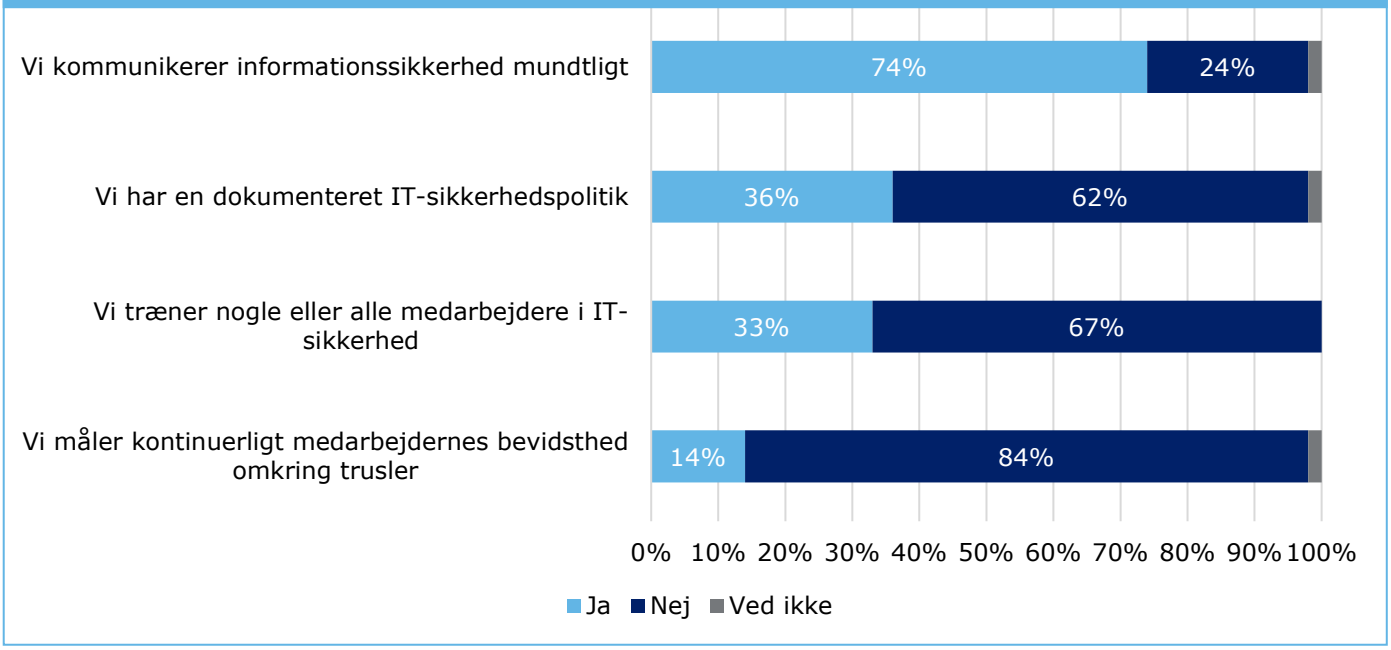
Kilde: Wilke for Monitor Deloitte

Der er også en stor del af virksomhederne, der ikke har implementeret andre grundlæggende IT-sikkerhedstiltag. Det drejer sig i særlig grad om IT-sikkerhedsanalyser og/eller IT-revision såvel som et dokumenteret overblik over kritisk information og systemer, hvor implementeringsgraden er lav. Ser man på tværs af de resterende grundlæggende IT-sikkerhedstiltag, er det kun gennemsnitligt 49 procent, der har implementeret disse (heri indregnes, at man enten har implementeret intern eller ekstern IT-sikkerhedsanalyse og/eller IT-revision).

Danske SMV'er bruger i høj grad ikke formaliserede tiltag i deres arbejde med IT-sikkerhed målrettet medarbejderne

Majoriteten af danske SMV'er har ikke en formaliseret tilgang til medarbejdernes bevidsthed, viden og kompetencer i forhold til IT-sikkerhed. Uformel kommunikation er det mest udbredte værktøj i relation til medarbejderne, som det fremgår af Figur 2.

Figur 2. Andel SMV'er, der har implementeret IT-sikkerhedstiltag målrettet medarbejderne



Kilde: Wilke for Monitor Deloitte

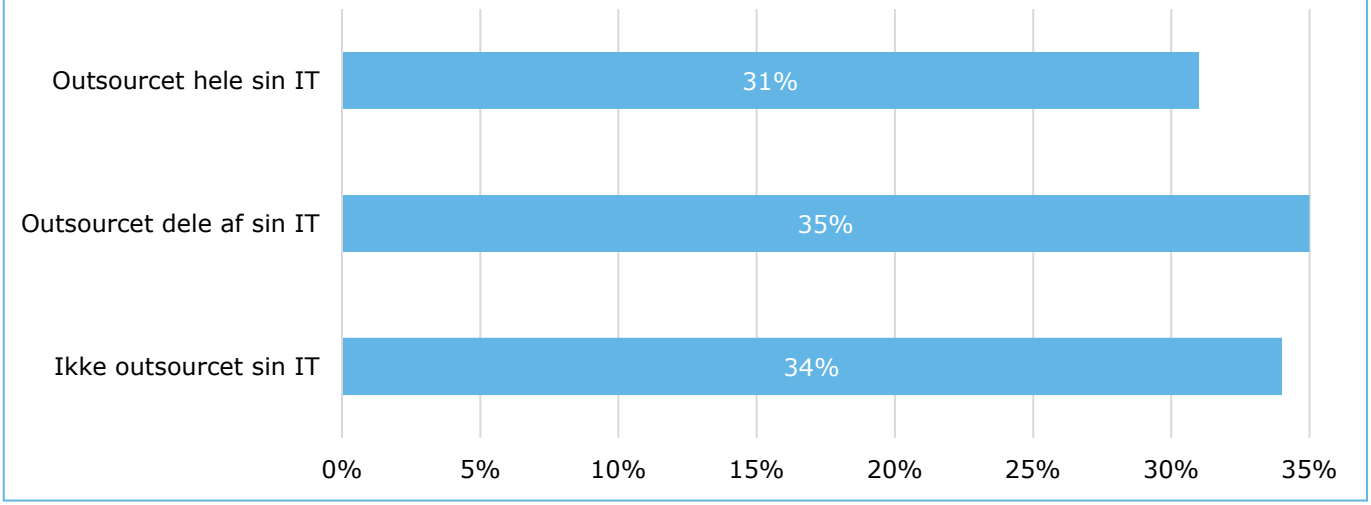
I modsætning til mundtlig kommunikation af IT-sikkerhed anvender en langt færre SMV'er mere formaliserede tiltag såsom formel træning, og særligt måling af medarbejdernes bevidsthed anvendes af meget få virksomheder.

Det er i særlig grad de mindre virksomheder, der anvender de ikke-formaliserede tiltag fremfor formaliserede tiltag. De små virksomheder anvender mundtlig kommunikation i cirka lige så høj grad som de større virksomheder, men kun 22 procent af virksomhederne med 5-9 ansatte har en dokumenteret IT-sikkerhedspolitik. Af virksomhederne med 5-9 ansatte er det også kun 15 procent, der træner alle medarbejdere, og 13 procent træner enkelte medarbejdere.

70 procent af SMV'erne har outsourcet hele eller dele af deres IT, hvilket har implikationer for IT-sikkerheden

For SMV'er kan det være fordelagtigt at outsource IT-infrastruktur og IT-systemer. Virksomheder kan benytte outsourcing i varierende grad fra outsourcing af enkelte dele af virksomhedens infrastruktur til fuld outsourcing af alle IT-relaterede opgaver. Årsager til, at virksomhederne benytter sig af outsourcing af IT, kan blandt andet være, at virksomhederne ikke har de fornødne kompetencer på området til selv at kunne etablere og drive den nødvendige infrastruktur. Det kan også være et ressourcespørgsmål, hvor de høje etableringsomkostninger erstattes af en månedlig ydelse til outsourcingpartneren.

Figur 3. Andel SMV'er, der har outsourcet deres IT



Kilde: Wilke for Monitor Deloitte

31 procent af de danske SMV'er har outsourcet hele deres IT, mens 35 procent har outsourcet dele af deres IT, som det fremgår af Figur 3.

Når man vælger at outsource hele eller dele af sin IT, er det vigtigt, at man stadig forholder sig til IT-sikkerhed. Til trods for dette er det kun 53 procent af de virksomheder, der har outsourcet hele deres IT, som har en databehandleraftale, mens tallet er 39 procent for de virksomheder, der har outsourcet dele af deres IT.

Som led i indeværende undersøgelse blev der gennemført 14 kvalitative caseinterviews[2]. 10 af virksomhederne i caseinterviewene har valgt at outsource hele eller dele af deres IT, og deres leverandør bliver dermed en vigtig faktor i og drivkraft for virksomhedens IT-sikkerhed. Alle disse virksomheder opfatter dette som en drivkraft for deres IT-sikkerhed, fordi de får adgang til flere kompetencer, og fordi deres IT-sikkerhed varetages af nogle, der har spidskompetencer indenfor IT. Virksomhederne ser derfor, at det kan øge deres IT-sikkerhed, at de anvender en outsourcingpartner. Som virksomhed bør man dog stille krav til sin leverandør vedrørende IT-sikkerhed, fordi leverandøren bliver afgørende for, at ens systemer og data er sikre. Man bør blandt andet stille krav til databehandling, backup, opdatering af systemer og andre grundlæggende IT-sikkerhedsforanstaltninger. Selvom man har valgt at outsource sin IT, er det vigtigt, at man stadig tager ansvar for sin IT-sikkerhed, selvom det kan være udfordrende at stille de nødvendige krav, fordi det kræver, at man tilegner sig viden og holder sig opdateret.

Virksomhedskulturen er en central barriere for SMV'ernes arbejde med IT-sikkerhed, og flere SMV'er arbejder med sikkerhedskulturen ved at øge videnniveauet blandt medarbejderne.
Af caseinterviewene fremgik det, at 10 af de 14 casevirksomheder oplever medarbejdernes handlinger og manglende viden om IT-sikkerhed som en barriere for virksomhedens arbejde med IT-sikkerhed. Ifølge virksomhederne kommer det blandt andet til udtryk ved, at medarbejderne udviser manglende imødekommenhed overfor de forandringer, der har været nødvendige for at øge IT-sikkerheden, og som samtidig påvirker medarbejdernes arbejdsgange. Derudover oplever virksomhederne også, at medarbejderne ikke i tilstrækkelig grad er i stand til at identificere IT-sikkerhedstrusler. Flere virksomheder nævner i den sammenhæng virksomhedskulturen som en underliggende barriere for at øge IT-sikkerhedsniveauet i virksomheden. Flere IT-ansvarlige mener, at det er nødvendigt at arbejde meget med kommunikationen om IT-sikkerhed og potentielle IT-sikkerhedstrusler for at kunne forankre IT-sikkerhed i virksomhedskulturen. Den uformelle kommunikation er i den sammenhæng et redskab til at skabe den nødvendige kulturforandring, og 74 procent af de danske SMV'er anvender også mundtlig kommunikation til medarbejderne i deres arbejde med IT-sikkerhed. Den uformelle kommunikation skaber et øget fokus på IT-sikkerhed og en forståelse af vigtigheden af IT-sikkerhed såvel som konsekvenserne ved manglende IT-sikkerhed for virksomheden. Derfor er det positivt, at så mange SMV'er anvender mundtlig kommunikation. I kommunikationen er det centralt, at medarbejderne kan forstå, hvad IT-sikkerhed er, og det er derfor nødvendigt at gøre IT-sikkerhed

[2] Se afsnit 2.2 for beskrivelse af brug af caseinterviews

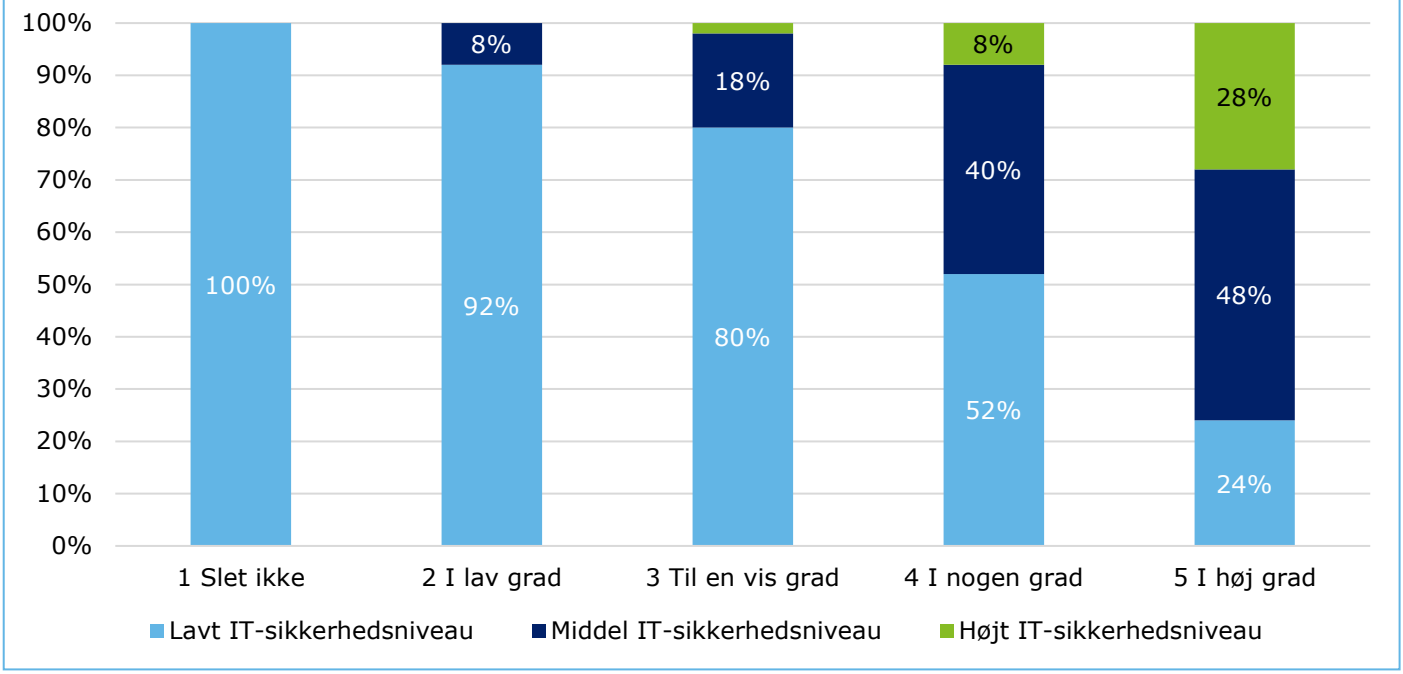
meget håndgribelig og kontekstuel og derudover målrette den mod de enkelte medarbejdergrupper. Dog er den mundtlige kommunikation ofte ikke nok, og det kan derfor være nødvendigt at følge op med mere formaliserede tiltag, så IT-sikkerhed også forankres i virksomhedens processer og arbejdsgange.

Ledelsens fokus på IT-sikkerhed øger IT-sikkerheden i de danske SMV'er

I mange virksomheder er ansvaret for IT-sikkerheden placeret hos virksomhedens IT-ansvarlige, men for at sikre et tilstrækkeligt IT-sikkerhedsniveau kræver det, at IT-sikkerhed også forankres i ledelsen for at sikre tilstrækkelig ressourcer. Flere af casevirksomhederne påpeger i denne sammenhæng ledelsens manglende engagement i IT-sikkerhed som værende en barriere for IT-sikkerheden i virksomheden. Årsagen hertil er todelt. Dels allokerer ledelsen dermed ikke tilstrækkelige ressourcer til virksomhedens IT-sikkerhed, dels har ledelsens manglende engagement en afsmittende effekt på virksomhedskulturen. For at øge ledelsens engagement i IT-sikkerhed og nedbryde den barriere, ledelsens manglende forståelse og engagement kan udgøre, er flere IT-chefer i virksomhederne begyndt at informere ledelsen om IT-sikkerhed og de eventuelle konsekvenser ved manglende IT-sikkerhed. Ligesom det er tilfældet med medarbejderne, kan det dreje sig om mundtlig kommunikation, hvor man kontinuerligt skubber information til ledelsen, hvilket hjælper med til at øge ledelsens fokus på området. Udover den mundtlige kommunikation påpeger flere af virksomhederne, at det også er værdifuldt at få udarbejdet en ekstern IT-sikkerhedsanalyse, da det gør det lettere at kommunikere IT-sikkerhed til ledelsen.

Når man ser på niveauet for ledelsens stillingtagen til IT-sikkerhed og virksomhedens IT-sikkerhedsniveau, ses der også en tendens til, at i jo højere grad ledelsen har taget stilling til IT-sikkerhed, jo højere er virksomhedens IT-sikkerhedsniveau, som det fremgår af Figur 4.

Figur 4. Sammenhængen mellem ledelsens stillingtagen til IT-sikkerhed og IT-sikkerhedsniveauet



Kilde: Wilke for Monitor Deloitte og Monitor Deloitte-analyse

Sammenhængen mellem ledelsens stillingtagen til IT-sikkerhed og IT-sikkerhedsniveauet indikerer, at ledelsens stillingtagen også kan være en drivkraft for IT-sikkerhedsniveauet. Årsagen til dette kan være, at når ledelsen har tilstrækkelig viden om IT-sikkerhed, forstår de behovet for IT-sikkerhed og kan derfor se nødvendigheden af at allokere ressourcer til indsatsen.

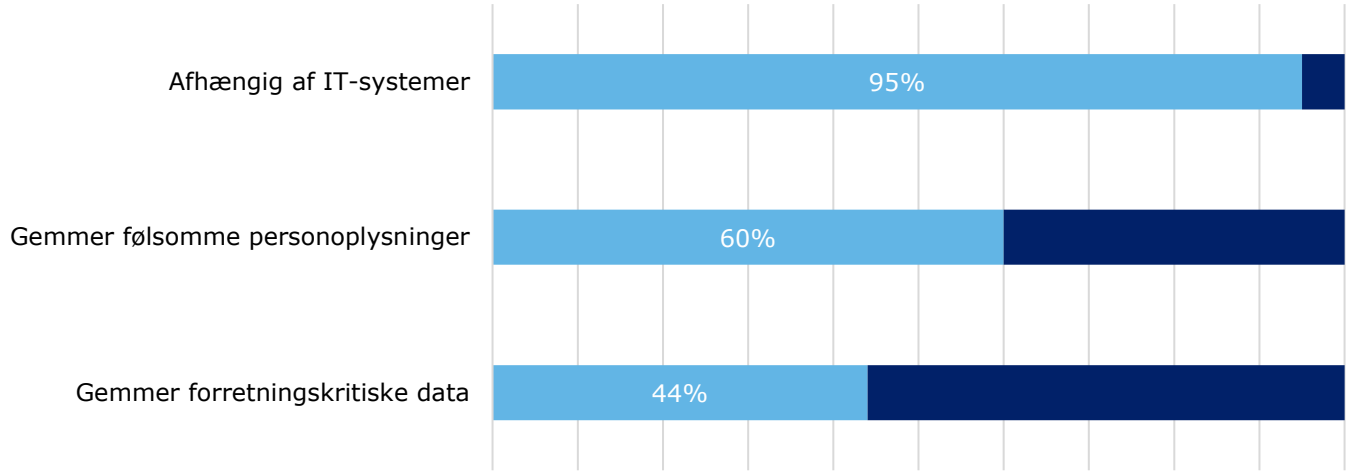
Viden om IT-sikkerhed er centralt for SMV'ernes arbejde med IT-sikkerhed
I flere virksomheder er det en barriere for igangsættelse af nødvendige IT-sikkerhedsforanstaltninger, at den IT-ansvarlige og de relevante beslutningstagere i virksomheden ikke har tilstrækkelig viden om blandt andet trusselsbilledet, og hvilke sikkerhedsmæssige tiltag der vil være relevante. Utilstrækkelig viden kan medføre, at virksomheden ikke får taget de forholdsregler, som dens risikoprofil tilsiger, og at virksomheden ikke rettidigt får reageret på og adresseret nye sikkerhedstrusler, i takt med at de opstår. 5 af de 14 casevirksomheder nævner, at professionelle og personlige netværk og fora kan være væsentlige kilder til viden om IT-sikkerhed. De forskellige fora kan være brancherelaterede, men kan også være mere tværgående.

Høj risikoprofil er en drivkraft for virksomhedernes IT-sikkerhedsniveau
For flere af casevirksomhederne er deres arbejde med IT-sikkerhed drevet af, at de ønsker at undgå nedbrud i deres IT. Dette er især tilfældet for virksomheder, hvor man har identificeret, at man har nogle meget kritiske systemer, som forretningen ikke kan fungere uden, og drivkraften for arbejdet med IT-sikkerhed er derfor relateret til virksomhedens risikoprofil. Da mange virksomheder samtidig ser, at når IT-trusselsbilledet øges, øges bekymringen for et IT-sikkerhedsbrud også, og man ønsker derfor at være proaktiv for at undgå dette. IT-trusselsbilledet bliver dermed også en drivkraft. Dermed gælder bekymringen de konsekvenser, et IT-sikkerhedsbrud kan have, men også den øgede risiko for et IT-sikkerhedsbrud som følge af et højere IT-trusselsbillede.

Et IT-sikkerhedsbrud øger SMV'ernes fokus på IT-sikkerhed
Oplever man som virksomhed et IT-sikkerhedsbrud, kan det blive en drivkraft for arbejdet med at øge IT-sikkerheden, fordi man oplever, hvor kritisk et sikkerhedsbrud kan være. 35 procent af virksomhederne i caseinterviewene har oplevet et IT-sikkerhedsbrud i større eller mindre grad og har oplevet, at det blev en drivkraft for deres arbejde med IT-sikkerhed. Det betød, at de udover at øge antallet af IT-sikkerhedsforanstaltninger også kunne bruge IT-sikkerhedsbruddet i kommunikationen internt til både ledelsen og medarbejderne. IT-sikkerhedsbruddet gjorde konsekvenserne meget håndgribelige for ledelsen og medarbejderne, fordi det blev klart, hvordan det påvirkede virksomheden, og dermed understregede det vigtigheden af IT-sikkerhed.

Konsekvenserne ved et IT-sikkerhedsbrud kan være vidtrækkende
Manglende IT-sikkerhed kan have omfangsrige konsekvenser for en virksomhed i tilfælde af et IT-sikkerhedsbrud og kan udover direkte økonomiske konsekvenser medføre langsigtede konsekvenser, der kan true virksomhedens eksistens.

Figur 5. SMV'ernes afhængighed af systemer samt opbevaring af data



Kilde: Wilke for Monitor Deloitte

Af Figur 5 fremgår det, at 95 procent af de adspurgte SMV'er er afhængige af deres IT-systemer i deres daglige drift, hvoraf 70 procent har en høj afhængighed. Omtrent 60 procent af SMV'erne gemmer følsomme personoplysninger, 44 procent gemmer forretningskritiske data, og små 20 procent af SMV'erne nævner, at læk af forretningskritiske data vil betyde, at de mister deres forretningsgrundlag og potentielt må dreje nøglen om. Et IT-

sikkerhedsbrud, der eksempelvis låser virksomhedens data eller giver adgang til centrale data, kan altså have vidtrækkende og skadende konsekvenser for mange danske SMV'er.

Undersøgelsen peger på, at de gennemsnitlige direkte omkostninger ved et IT-sikkerhedsbrud ligger på cirka 40.000 kr. Af de virksomheder, der har haft et IT-sikkerhedsbrud inden for det sidste år svarer cirka en sjettedel, at omkostningerne løb op i 100.000-200.000 kr. Omkostningsestimater er dog også præget af mørketal, dels fordi det ikke er oplysninger, man ønsker at dele, dels på grund af virksomhedernes manglende bevidsthed om det fulde omfang af konsekvenserne ved et IT-sikkerhedsbrud. De direkte omkostninger ofte blot toppen af isbjerget, og de indirekte omkostninger, der ligger under overfladen, kan påvirke en virksomhed langt ud i fremtiden. Det kan betyde, at virksomheden mister kommercielle muligheder på grund af forringet image, eller at virksomheden mister centrale data gennem erhvervsspionage, hvor bagmanden ønsker at få adgang til forretningskritiske data for enten at kopiere virksomhedens produkt eller sælge informationen videre.

Andre kilder estimerer de gennemsnitlige omkostninger ved et IT-sikkerhedsbrud til at ligge på et andet niveau:

- PwC, Cybercrime Survey 2017: 900.000 kr.
- Kaspersky: 3.300.000 kr.

IT-sikkerhed anvendes i dag ikke som konkurrenceparameter

Da IT-sikkerhed kan betyde meget for virksomhederne, kan det også være noget, de bruger som konkurrenceparameter. I caseinterviewene viser det sig dog, at kun en enkelt af virksomhederne har brugt IT-sikkerhed som konkurrenceparameter, og derudover viste resultater fra spørgeskemaundersøgelsen, at kun 15 procent har implementeret IT-sikkerhedsforanstaltninger af kommercielle årsager. Adspurgte eksperter ser dog, at der er sket en udvikling på området, der går imod, at flere ser IT-sikkerhed som en mulig konkurrenceparameter, hvilket også afspejles i, at det ikke længere kun er IT-chefen, der forholder sig til IT-sikkerhed, men også resten af ledelsen og endda bestyrelsen. Det er dog stadig i lav grad, og det er primært i brancher, hvor der er særlig regulering, eller hvor virksomhederne netop sælger IT-sikkerhedsløsninger.

2 Baggrund for rapporten

Redegørelsen for Danmarks Digitale Vækst 2017 konkluderede, at mindre virksomheder halter bagefter i forhold til de store virksomheder, når det gælder IT-sikkerhed. Virksomhedsrådet for IT-sikkerhed har i deres anbefalinger fra marts 2017 blandt andet peget på, at virksomheder mangler viden om aktuelle IT-sikkerhedstrusler, potentielle konsekvenser af IT-sikkerhedsangreb og relevante tiltag til at beskytte deres IT-systemer og data. Det gælder ikke mindst små og mellemstore virksomheder uden egen IT-afdeling. IT-sikkerhed er et centralt område, og Erhvervsstyrelsen ønsker viden om status for IT-sikkerhed i danske SMV'er.

Monitor Deloitte har for Erhvervsstyrelsen udarbejdet et statusbillede af IT-sikkerhedsniveauet i danske SMV'er. Dette er sket med henblik på at kortlægge, om danske SMV'er har et tilstrækkeligt IT-sikkerhedsniveau, og om de har tilpasset deres indsatser på området.

2.1 Formål

Analysen har til formål at skabe kvalificeret viden om danske SMV'ers IT-sikkerhed og databeskyttelse. Besvarelsen af fire centrale spørgsmål har været retningsskabende for analysen:

1. I hvilken grad besidder danske SMV'er viden og kompetencer på området?
2. I hvor høj grad har virksomhederne iværksat IT-sikkerhedsforanstaltninger og -processer og foretaget investeringer i IT-sikkerhed?
3. Hvad er et passende IT-sikkerheds- og databeskyttelsesniveau i virksomhederne?
4. Hvilke barrierer og drivkræfter påvirker virksomhederne ifm. implementering af IT-sikkerhed?
5. Hvad er konsekvenserne for virksomhederne ved ikke at have tilstrækkelig IT-sikkerhed?

2.2 Metode og datakilder

Monitor Deloitte har anvendt en række forskellige datakilder, som det fremgår af Tabel 2. Datakilderne understøtter og supplerer hinanden og muliggør triangulering af de forskellige konklusioner på tværs af datakilderne. Årsagen til denne sekventielle udførelse var at sikre, at konklusioner og hypoteser fra de forskellige stadier blev viderebragt til næste niveau for løbende at tilpasse analysearbejdet. Således blev spørgeskemaundersøgelsen først udviklet og gennemført. Dernæst blev spørgeguide til caseanalyserne udviklet. I forbindelse med at besvarelserne fra spørgeskemaundersøgelsen kom retur, blev selve caseinterviewene udført. Afsluttende blev de resterende datakilder brugt.

Tabel 2. Datakilder anvendt til at afdække problemet

Datakilder

- **Telefonbaseret spørgeskemaundersøgelse:** Spørgeskemaundersøgelsen, der er udviklet af Monitor Deloitte, blev gennemført af Wilke og omfattede 1.054 besvarelser fordelt på 18 forskellige brancher i Danmark. Det store antal respondenter i undersøgelsen gjorde, at undersøgelsen kunne drage generelle konklusioner om såvel SMV-segmentet som helhed som om enkelte udvalgte industrier med høj statistisk nøjagtighed. Spørgeskemaundersøgelsen bestod af 25 spørgsmål, der kortlagde viden-, kompetence- og foranstaltningsniveauet i de udvalgte virksomheder. Spørgeskemaundersøgelsen blev gennemført i uge 41-45 i 2017.
- **Caseanalyser:** Baseret på resultaterne fra spørgeskemaundersøgelsen er caseanalyserne anvendt til at give dybere indsigt i virksomhedernes arbejde med IT-sikkerhed. Caseanalyserne er baseret på 14 virksomhedsinterview med de IT-ansvarlige i de pågældende virksomheder. Virksomhederne er udvalgt med henblik på at repræsentere forskellige brancher, virksomhedsstørrelser og dele af det identificerede udfaldsrum i spørgeskemaundersøgelsen. Caseanalyserne er gennemført i uge 43-45 i 2017. Alle caseinterview er beskrevet i bilagene. Ni af virksomhederne ønskede at være anonyme, og her er der derfor brugt aliasser for at skjule virksomhedernes rigtige navne.
- **DST VITA:** Danmarks Statistik (DST) udgiver årligt deres analyse af danske virksomheders IT-anvendelse (VITA). Analysen baseres på en større webbaseret spørgeskemaundersøgelse, hvor cirka 3.500 danske virksomheder deltager. Datagrundlaget fra 2015- og 2016-analyserne er i denne rapport blevet brugt til at be- eller afkræfte hypoteser fra spørgeskemaundersøgelsen og caseanalyserne.
- **Hackersimuleringer:** Baseret på over 50.000 simulerede hackerangreb foretaget af Deloitte Cyber Risk i knap 600 danske virksomheder er disse aggregerede data brugt til at be- eller afkræfte hypoteser på samme måde som DST VITA. Datagrundlaget for hackersimuleringerne er særlig unikt og er ikke anvendt før i en dansk kontekst.
- **Litteratur:** Der er foretaget en gennemgang af empirisk litteratur på området. Fokus har været på studier, hvor Danmarks IT-sikkerhedsniveau er blevet sammenlignet med andre lande, og på studier, hvor den aktuelle IT-trussel og udviklingen heri er blevet analyseret. Litteraturen er specielt anvendt i kapitel 3 og 6.
- **Ekspertinterview:** Som supplement til litteraturstudiet er emnespecifikke eksperter blevet interviewet for primært at få deres vurdering af henholdsvis konsekvenser og konkurrencemæssige fordele/ulemper ved et øget IT-sikkerhedsniveau i danske SMV'er. Eksperterne er: Kim Schlyter (partner i Deloitte Cyber Risk), Ole Kjeldsen (bestyrelsesmedlem i Rådet for Digital Sikkerhed, og CTO & CISO i Microsoft) og Michael Appelby (General Manager i ZyberSafe)

Det metodiske grundlag fremgår i detaljer af appendiks 7.1 og 7.3.

2.3 Læsevejledning

Rapporten er struktureret efter tre overordnede analysetemaer:

- **Kapitel 3. IT-sikkerhed i Danmark:** Kapitlet giver en kort redegørelse for Danmarks nuværende IT-sikkerhedsniveau sammenlignet med andre lande. Dernæst klarlægger kapitlet trusselsbilledet indenfor IT-kriminalitet i dag, og desuden præsenterer det en tilgang til vurdering af IT-sikkerheden i danske SMV'er.
- **Kapitel 4. Status for IT-sikkerhed for danske SMV'er:** Kapitlet afdækker status for IT-sikkerhed i danske SMV'er og går i dybden med SMV'ernes IT-sikkerhed indenfor tre områder: medarbejdere og ledelse, IT-sikkerhedsforanstaltninger og fysisk adgangskontrol. Til slut sammenholdes SMV'ernes IT-sikkerhedsniveau med risikoprofilen for at vurdere, om IT-sikkerhedsniveauet er tilstrækkeligt i danske SMV'er.
- **Kapitel 5. Barrierer og drivkræfter for at øge IT-sikkerhedsniveauet i danske SMV'er:** Baseret på resultater fra kapitel 3 dykkes der i kapitel 4 længere ned i de drivkræfter, der gør, at SMV'er øger deres IT-sikkerhedsniveau, og de barrierer, der holder dem tilbage i forhold til at øge deres IT-sikkerhedsniveau. Kapitlet baseres på 14 kvalitative interview med udvalgte danske SMV'er.
- **Kapitel 6. Negative og positive konsekvenser ved IT-sikkerhed:** Det afsluttende kapitel perspektiverer resultaterne fra de foregående kapitler, så der ses på de konsekvenser, et manglende IT-sikkerhedsniveau kan have, og på det fremadrettede konkurrencepotentiale i et øget IT-sikkerhedsniveau for Danmark som helhed.

2.4 Begrebsafklaring

I dette afsnit klarlægges de centrale begreber, der anvendes i rapporten.

IT-sikkerhed
En samlet betegnelse for de tiltag og foranstaltninger, som organisationer gør for at forhindre IT-sikkerhedsbrud og minimere de negative følgevirkninger af et brud ved hurtigt at kunne genoprette systemer eller data.

IT-sikkerhedsangreb
Et kriminelt forsøg på at kompromittere en virksomheds systemer og data, for eksempel med det formål at få adgang til kritiske data eller få en løsesum for krypterede data.

IT-sikkerhedsbrud
Et succesfuldt IT-sikkerhedsangreb, hvor hackere uretmæssigt skaffer sig adgang til en virksomheds systemer eller data.

IT-sikkerhedshændelse
En fælles betegnelse, der omfatter både IT-sikkerhedsangreb og IT-sikkerhedsbrud.

IT-sikkerhedsniveau
Det samlede niveau for virksomhedens IT-sikkerhed og dermed mængden af tiltag og foranstaltninger, virksomheden har gjort i relation til virksomhedens IT-sikkerhed.

IT-sikkerhedsforanstaltninger
Konkrete tekniske foranstaltninger relateret til virksomhedens IT, som virksomheden har gjort med henblik på at øge virksomhedens IT-sikkerhed.

Formaliserede tiltag
Tiltag relateret til virksomhedens medarbejdere, der ofte vil være skriftligt dokumenteret og/eller struktureret, for eksempel en IT-sikkerhedspolitik.

Ikke-formaliserede tiltag
Tiltag relateret til virksomhedens medarbejdere, der ofte foregår løbende og i mindre formel form, for eksempel mundtlig kommunikation.

IT-sikkerhedsanalyse
En analyse foretaget af enten en ekstern partner eller af virksomheden selv, der vurderer virksomhedens IT-sikkerhed og har til formål at klarlægge, om virksomheden har brister i deres IT-sikkerhed.

Drivkraft
Bagvedliggende årsag eller incitament til, at virksomhederne løfter deres IT-sikkerhedsniveau.

Barriere
Bagvedliggende årsag til eller hindring for, at virksomhederne ikke evner eller vælger at løfte deres IT-sikkerhedsniveau.

Risikoprofil
Angiver en samlet vurdering af, hvor alvorligt et IT-sikkerhedsbrud vil være for virksomheden, og hvor stor sandsynligheden er for, at virksomheden bliver ramt. Dette er en kombination af flere parametre, herunder virksomhedens afhængighed af IT-systemer, om virksomheden har forretningskritiske eller følsomme data (følsomme personoplysninger) og virksomhedens branche.

Essentielle IT-sikkerhedsforanstaltninger (essentielle tiltag)
Omfatter dokumenteret og gennemtestet backupprocedure og løbende opdateringer af systemer og programmer. Antivirusprogram og firewall anses også som essentielle IT-sikkerhedsforanstaltninger, men udelades i denne undersøgelse, da disse ofte er indbygget som standard i virksomhedernes styresystemer og hardware.

Grundlæggende IT-sikkerhedsforanstaltninger (grundlæggende tiltag)
Omfatter de essentielle IT-sikkerhedsforanstaltninger, og om virksomheden derudover har f.eks. en fast procedure for håndtering af følsomme personoplysninger eller løbende vurdering af og opfølgning på medarbejderadgange.

Avancerede IT-sikkerhedsforanstaltninger (avancerede tiltag)
Avancerede tiltag omfatter overvågning og logning af systemer, samarbejdsaftale med eksterne leverandører, forsikringspolice, der dækker i tilfælde af IT-sikkerhedsbrud, databehandleraftale og dokumenteret beredskabsplan.

IT-trusselsbillede
Den samlede IT-trussel fra IT-kriminelle. IT-trusselsbilledet er en samlet betegnelse for de IT-sikkerhedstrusler, der er mod virksomheden.

3 IT-sikkerhed i Danmark

Danmark har historisk set haft et højt digitaliseringsniveau sammenlignet med andre lande. Men IT-sikkerhedsniveauet er ikke tilsvarende højt, og der er tegn på, at Danmark har et lavere IT-sikkerhedsniveau end de lande, vi normalt sammenligner os med.

3.1 Danske virksomheder og myndigheder er langt fremme med digitalisering sammenlignet med andre europæiske lande

I takt med at danske virksomheder og myndigheder øger deres grad af digitalisering og afhængighed af internettet, stiger truslen for IT-sikkerhedsangreb ligeledes. Digitalisering skaber mange muligheder for innovation på virksomheds- og myndighedsniveau, men øger samtidig risikoen for IT-sikkerhedsangreb.

Danmark er langt fremme, hvad angår digitalisering. Dette gælder for både danske virksomheder og myndigheder. Danmarks Statistik udgav i 2016 en sammenligning af IT-anvendelsesgraden i Danmark og 12 europæiske lande.[3] Sammenligningen viste, at danske virksomheder i høj grad benytter sig af digitale løsninger sammenlignet med andre europæiske lande. Et par uddrag fra denne sammenligning er, at:

- 93 procent af danske virksomheder har en hjemmeside mod et gennemsnit i EU på 77 procent.
- 64 procent af danske virksomheder benytter sociale medier mod et gennemsnit i EU på 45 procent.
- 29 procent af danske virksomheder benytter e-salg mod et gennemsnit i EU på 20 procent.
- 43 procent af danske virksomheder gør brug af cloud computing mod et gennemsnit i EU på 20 procent.
- 72 procent af danske virksomheder har sendt eller modtaget e-faktura mod et gennemsnit i EU på 35 procent.

IT-anvendelsen i danske virksomheder er altså højere end EU-gennemsnittet og blandt toppen i Europa. Danmark ligger dog ikke blot højt i anvendelsen af IT – ifølge Europa-Kommissionens indeks for den digitale økonomi og det digitale samfund (DESI) fra 2017 er Danmark det land i EU, der har den mest digitaliserede økonomi.

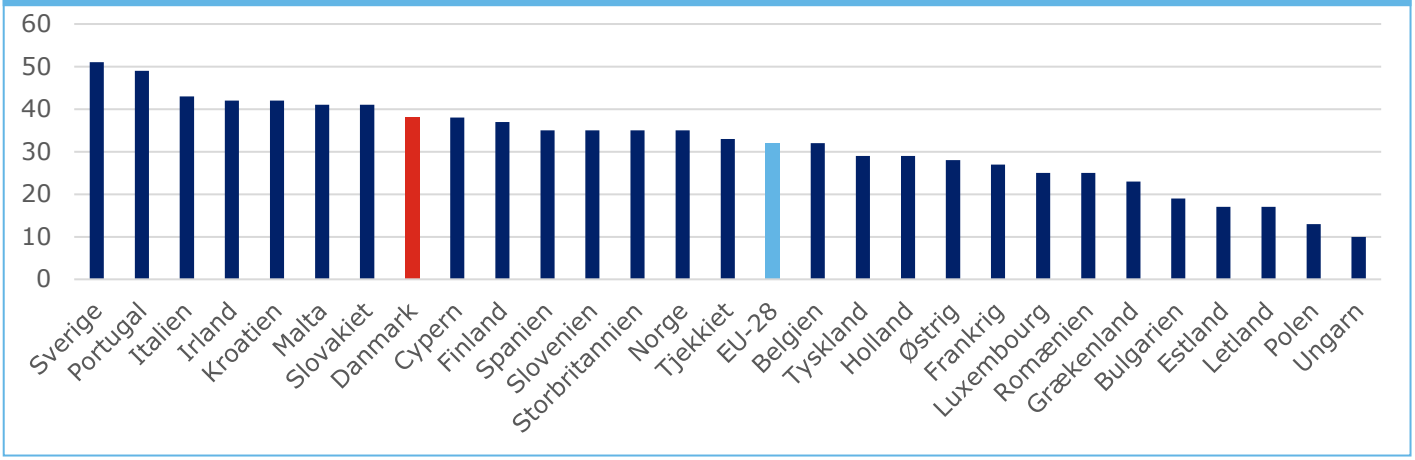
3.2 IT-sikkerheden i danske virksomheder har ikke fulgt med den høje digitaliseringsgrad

Det er centrale spørgsmål, om IT-sikkerheden i danske virksomheder matcher den høje grad af digitalisering, og om virksomhederne i tilstrækkelig grad er i stand til at beskytte sig mod IT-sikkerhedsangreb.

Eurostat har i 2015 indsamlet svar på IT-relaterede spørgsmål på tværs af hele EU. Tages der i den undersøgelse udgangspunkt i den andel af virksomheder, der har formaliseret en IT-sikkerhedspolitik, ligger Danmark nummer 8 ud af 28 lande, jf. Figur 6.

[3] http://www.dst.dk/Site/Dst/Udgivelser/GetPubFile.aspx?id=28382&sid=itvirkeu2016

Figur 6. Andel virksomheder i EU-28 med en formel IT-sikkerhedspolitik, 2015



Kilde: Eurostat
Note: Ingen data tilgængelige for Litauen. Norge er medtaget, selvom de ikke er del af EU-28.

3.3 IT-trusselsbilledet for danske virksomheder er voksende og udvikler sig løbende

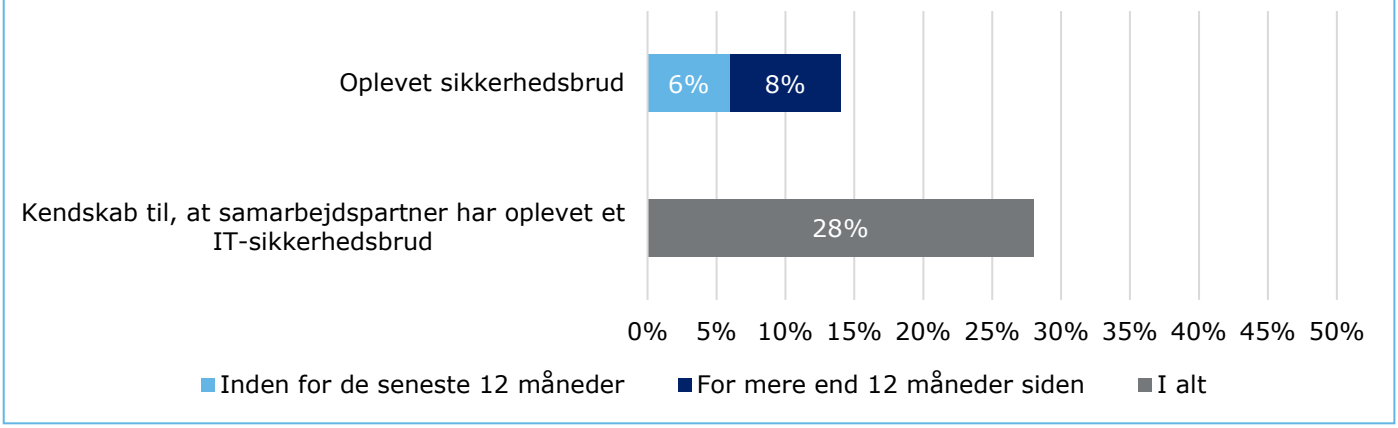
Sætter man Danmarks høje digitaliseringsgrad i perspektiv med, at IT-teknologien udvikler sig meget hurtigt, betyder det et større og større IT-trusselsbillede for Danmark, og truslen er under konstant forandring. Dette stiller høje krav til myndighedernes og ikke mindst virksomhedernes tilgang til IT-sikkerhed og datahåndtering. Dette har senest været kraftigt belyst i medierne med Mærsks IT-nedbrud i juli 2017, hvor Mærsks interne systemer ifølge Mærsks finansdirektør, Jakob Stausholm, blev låst i flere uger og medførte mere end 1,6 mia. kr. i tabt indtjening[4]. I trusselsvurderingen fra februar 2017 vurderer Center for Cybersikkerhed (CFCS), at truslen mod Danmark er meget høj, specielt i forhold til IT-spionage og IT-kriminalitet rettet mod både myndigheder, virksomheder og privatpersoner. CFCS nævner desuden, at der igennem de seneste år har været en stigning i antallet af IT-sikkerhedsangreb og dermed forsøg på at kompromittere danske virksomheder og myndigheder.[5]

IT-sikkerhedsniveauet i danske virksomheder er dog ikke blandt de bedste i Europa, og det øger virksomhedernes sårbarhed overfor IT-sikkerhedsangreb. Indeværende undersøgelse viser da også, at 14 procent af danske SMV'er har haft et decideret IT-sikkerhedsbrud, som det fremgår af Figur 7. Et IT-sikkerhedsbrud er et IT-sikkerhedsangreb, der lykkes. Et IT-sikkerhedsangreb er et forsøg på at ramme virksomheden og er derfor ikke nødvendigvis et tilfælde, hvor virksomhedens systemer eller data er blevet påvirket.

[4] https://www.dr.dk/nyheder/indland/maersk-cyberangreb-har-slaaet-indtjeningen-tilbage

[5] https://fe-ddis.dk/cfcs/CFCSDocuments/Cybertruslen%20mod%20Danmark.pdf

Figur 7. Antal SMV'er, der har oplevet et IT-sikkerhedsbrud



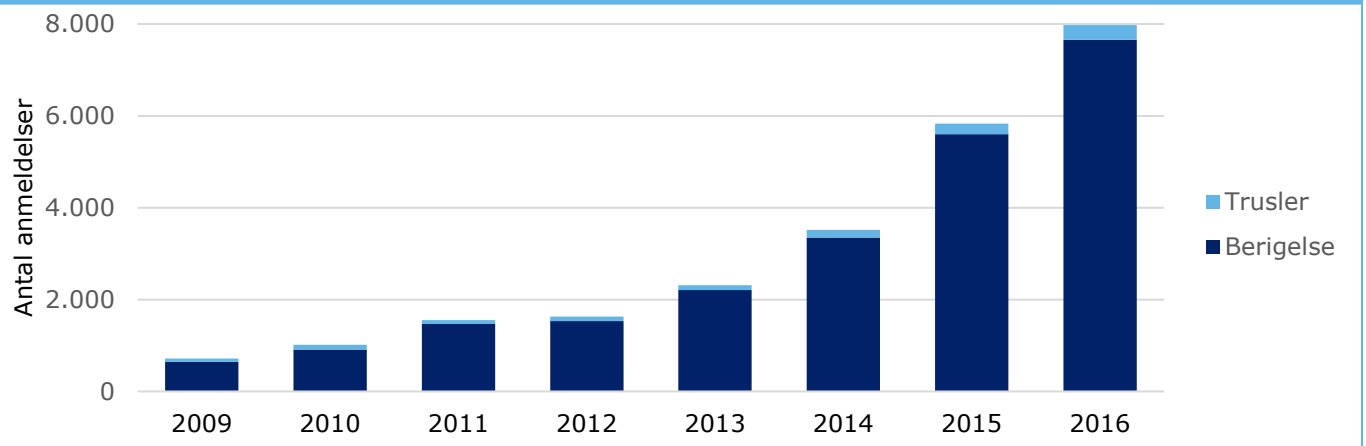
Kilde: Wilke for Monitor Deloitte

14 procent af danske SMV'er i denne undersøgelse har således haft et IT-sikkerhedsbrud, hvor virksomhedens daglige drift blev påvirket, fordi IT-systemer eller data blev skadet eller gjort utilgængelige. Dertil har 28 procent af SMV'erne kendskab til, at en samarbejdspartner har haft et IT-sikkerhedsbrud. IT-sikkerhedshændelser er dog forbundet med store mørketal, som det beskrives i næste afsnit. Flere ting tyder dog på, at virksomhederne er opmærksomme på det øgede trusselsbillede, idet de er mere bekymrede for IT-sikkerhedsbrud end for et år siden, som det fremgår af PwC's undersøgelse. PwC udgiver årligt deres Cybercrime Survey, hvor cirka 300 virksomhedsledere spørges om deres syn på forskellige IT-sikkerhedsforhold. I 2017 har 74 procent af respondenterne angivet, at de er mere bekymrede for IT-trusler nu end for 12 måneder siden. Dette tal var 65 procent i samme undersøgelse fra 2016.[6] PwC's undersøgelse viser, at cirka 70 procent af virksomhederne har været udsat for et IT-sikkerhedsangreb, hvilket ligeledes giver udtryk for, at IT-sikkerhedstruslen er høj.

Frygten i de danske virksomheder er begrundet, hvis man ser på tal fra dansk politi. Disse indikerer en stigende tendens i antallet af anmeldelser relateret til IT-berigelseskriminalitet, der dækker både borgerrettede og virksomhedsrettede anmeldelser, jf. Figur 8.

[6] https://www.pwc.dk/da/nyt/publikationer/cybercrime-survey-2017.html

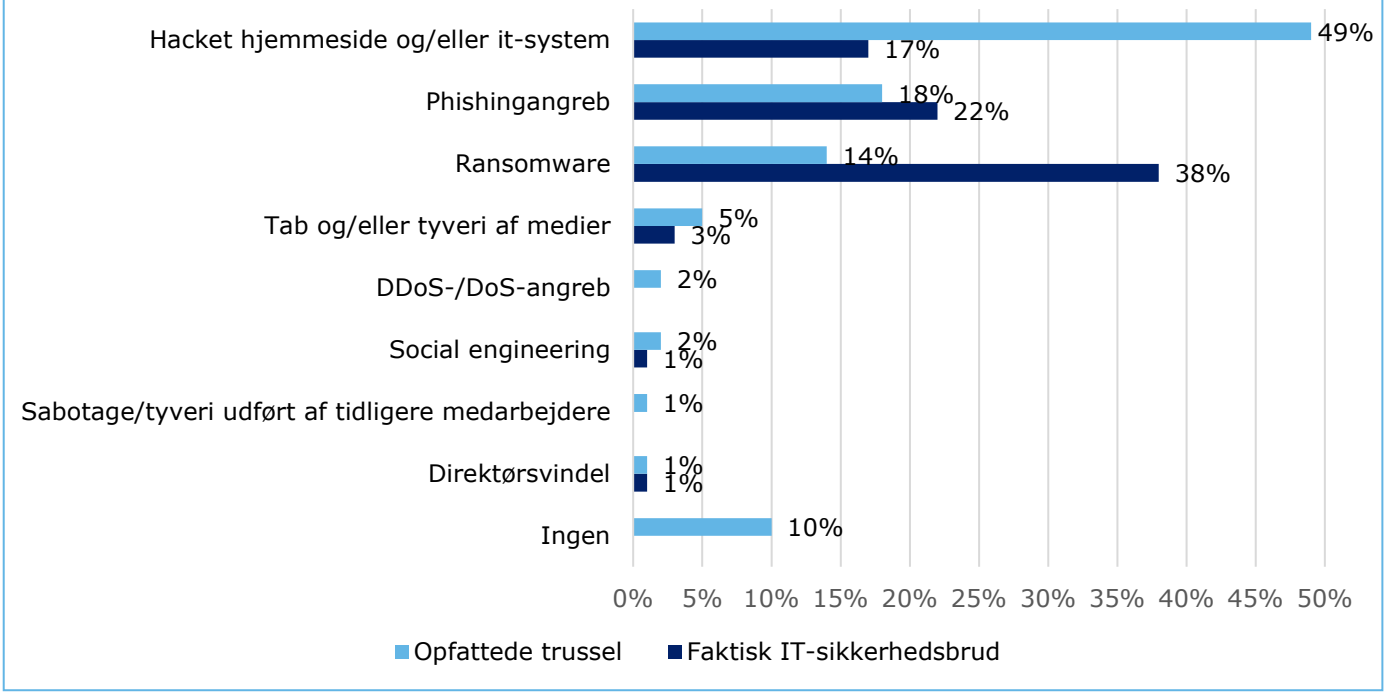
Figur 8. Antal anmeldelser af IT-relateret berigelseskriminalitet



Kilde: Politiet[7]
Note: Opgjort ved søgning på specifikke ordkombinationer i POLSAS 1. januar 2017.

Spørger man de danske SMV'er om deres vurdering af, hvad de væsentligste IT-trusler er, svarer majoriteten, at hacket hjemmeside og/eller IT-system såvel som phishingangreb ligger højest. Dette kan ses i Figur 9. Det er i den forbindelse også interessant, at 10 procent af virksomhederne ikke ser nogen IT-sikkerhedstrusler som væsentlige, hvilket kan være et tegn på, at nogle virksomheder ikke er tilstrækkelig opmærksomme på truslen fra IT-kriminelle.

Figur 9. SMV'ernes vurdering af IT-sikkerhedstrusler og de faktiske IT-sikkerhedsbrud



Kilde: Wilke for Monitor Deloitte

[7] https://www.politi.dk/NR/rdonlyres/60D84675-DFA7-46FE-BDEC-6FE6545FC8AF/0/Rapport_NSA17_enkeltsider.pdf

Sammenligner man SMV'ernes vurdering af de væsentligste IT-sikkerhedstrusler med de faktiske angreb i SMV'erne, ses ikke et entydigt billede i forhold til det opfattede og oplevede IT-trusselsbillede. Denne undersøgelse peger på, at den primære type IT-sikkerhedsbrud var ransomware, som 38 procent oplevede, hvor virksomhedens filer bliver krypteret. Til trods for at det mest typiske IT-sikkerhedsangreb var ransomware, var det kun 14 procent af SMV'erne, der så det som den væsentligste IT-sikkerhedstrussel, jf. Figur 9. 22 procent af dem, der oplevede et sikkerhedsbrud, oplevede det som en følge af et phishingangreb, hvor afsender udgiver sig for at være en anden for enten at få modtager til at give sine loginoplysninger eller downloade en fil. 18 procent af SMV'erne ser dette som den væsentligste IT-sikkerhedstrussel.

Ovenstående peger således på, at det opfattede IT-trusselsbillede er diffust i forhold til de IT-sikkerhedsangreb, virksomhederne oplever. Desuden peger det på, at selvom der er kommet øget fokus på IT-sikkerhed i medierne, er der stadig en stor del af SMV'erne, der ikke har tilstrækkelig viden på området.

3.4 Mørketal skjuler det reelle omfang af IT-trusselsbilledet

IT-trusselsbilledet og det aktuelle omfang af IT-sikkerhedshændelser i Danmark er kompliceret at afdække. Dette skyldes blandt andet, at man som virksomhed enten ikke har interesse i at dele med andre, hvis man har været udsat for et IT-sikkerhedsangreb, eller at man simpelthen ikke er bevidst om, at man har været udsat for et angreb. Dette kan være tilfældet, hvis der er tale om erhvervsspionage, hvor bagmanden ønsker at slippe uset ind i virksomhedens systemer.

Det er derfor usikkert, om det er fuldstændig retvisende, at kun 14 procent af de danske SMV'er har haft et IT-sikkerhedsbrud, mens 28 procent har kendskab til, at en samarbejdspartner har haft et sikkerhedsbrud. Udover at man ikke ønsker at dele, hvis man har haft et IT-sikkerhedsbrud, kan manglen på et fælles begrebsapparat gøre det svært at vurdere, hvornår et IT-sikkerhedsangreb bliver til et IT-sikkerhedsbrud, og dette slører det præcise tal yderligere.

Ser man på de kvalitative interview, der er gennemført i forbindelse med denne undersøgelse, har 35 procent af de 14 virksomheder haft et IT-sikkerhedsbrud. I den kvalitative del er der tale om interview, hvor der kan være opnået en større tillid, der kan have haft betydning for virksomhedernes villighed til at dele deres oplevelser. Virksomhederne i den kvalitative del af undersøgelsen er ikke repræsentative for den samlede population af danske SMV'er, men det kan give en formodning om, at niveauet for IT-sikkerhedsbrud kan være højere. Derfor er det svært at anslå det nøjagtige antal IT-sikkerhedshændelser i Danmark på årsbasis. Denne usikkerhed benævnes mørketal i litteraturen. Oplevede virksomheden i stedet en brand eller et indbrud, ville den i højere grad dele dette med sit netværk, hvilket ikke ses i samme omfang med IT-sikkerhedsbrud.

At det er svært at estimere antallet af IT-sikkerhedsangreb og IT-sikkerhedsbrud i Danmark understøttes også af en undersøgelse foretaget af Deloitte og Epinion i 2017. Undersøgelsen gik i detaljer med, hvordan danske virksomheder håndterer IT-sikkerhedsangreb. I denne undersøgelse, der er baseret på besvarelser fra 150 virksomheder i Danmark, svarer 24 procent af virksomhederne, at de indenfor det seneste år har haft et IT-sikkerhedsbrud i form af ransomware, der krypterede mindst én fil. Dette tal er væsentlig højere end de 14 procent, som denne undersøgelse peger på. Samtidig er der blot tale om en specifik type IT-sikkerhedsangreb.

De forskellige undersøgelser peger på meget forskellige niveauer for mængden af IT-sikkerhedsbrud i Danmark, hvilket understreger, at det er meget udfordrende at kvantificere mængden af IT-sikkerhedsbrud. Det indikerer samtidig, at der er et yderligere behov for at belyse omfanget af IT-sikkerhedsbrud i Danmark, fordi konsekvenserne kan være substantielle for virksomhederne. Øget belysning af området kan derfor være med til at mindske usikkerheden om omfanget og samtidig øge fokus på og forståelse af IT-sikkerhed.

4 Status for IT-sikkerhed for danske SMV'er

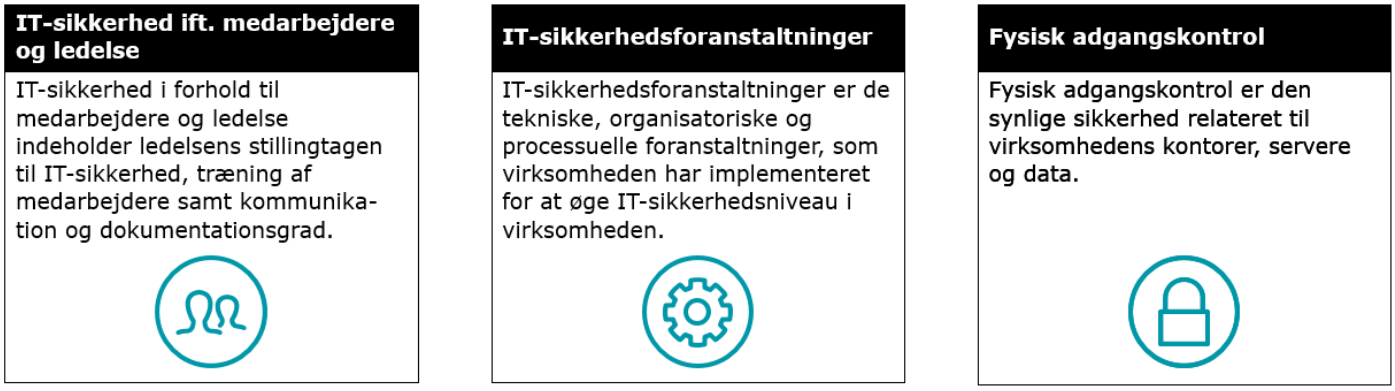
Indeværende undersøgelse viser, at over halvdelen af danske SMV'er har et lavt IT-sikkerhedsniveau. Der er dog generelt stor variation i danske SMV'ers IT-sikkerhed, idet der på den ene side er en stor del, der ikke har implementeret helt essentielle IT-sikkerhedstiltag, og på den anden side er der samtidig en stor gruppe, der har implementeret mere avancerede IT-sikkerhedstiltag.

Med udgangspunkt i den gennemførte spørgeskemaundersøgelse blandt 1.054 danske SMV'er afdækker dette kapitel IT-sikkerhedsniveauet i danske SMV'er og giver indsigt i, hvor SMV'erne klarer sig godt, og hvor de klarer sig mindre godt.

Indledningsvist præsenteres de overordnede resultater for IT-sikkerhedsniveauet, hvorefter de enkelte elementer i virksomhedernes IT-sikkerhedsniveau afdækkes. Til sidst vurderes SMV'ernes IT-sikkerhedsniveau ved at holde det op imod risikoprofilen. Dette viser, hvordan SMV'erne har tilpasset deres IT-sikkerhedsniveau til deres risikoprofil.

4.1 Majoriteten af danske SMV'er har et lavt IT-sikkerhedsniveau

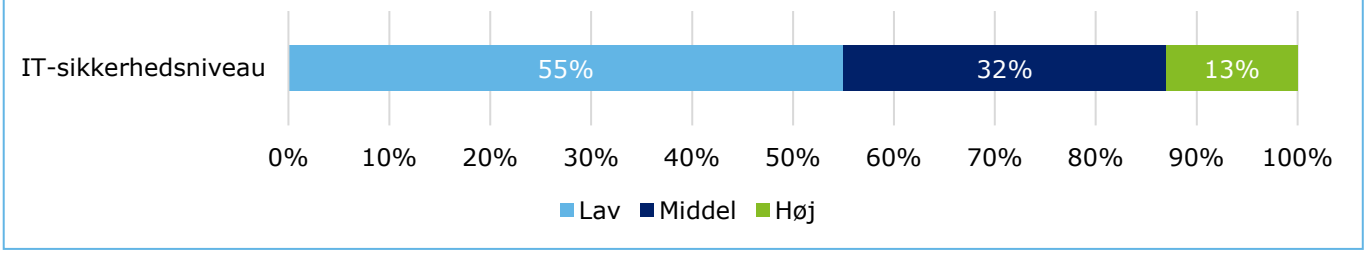
Når man vurderer en virksomheds IT-sikkerhedsniveau, vurderer man på tre parametre: IT-sikkerhed relateret til medarbejdere og ledelse, IT-sikkerhedsforanstaltninger og fysisk adgangskontrol. Disse er beskrevet i Figur 10 nedenfor.



Figur 10. Beskrivelse af parametre indeholdt i vurderingen af virksomhedernes IT-sikkerhedsniveau
Kilde: Monitor Deloitte og Deloitte Cyber Risk

Ser man på SMV'ernes IT-sikkerhedsniveau, har størstedelen af virksomhederne et lavt IT-sikkerhedsniveau, som det fremgår af Figur 11.

Figur 11. SMV'ernes IT-sikkerhedsniveau



Kilde: Wilke for Monitor Deloitte og Monitor Deloitte-analyse

Over halvdelen af danske SMV'er har et lavt IT-sikkerhedsniveau, mens kun 13 procent kan kategoriseres som havende et højt IT-sikkerhedsniveau.

Dette resultat understøttes af resultater fra flere andre kilder. Deloitte Cyber Risk har siden 2012 gennemført flere tusinde hackersimuleringer i mere end 550 danske virksomheder. I disse simuleringer har 57 procent af virksomhederne haft yderst kritiske sårbarheder i deres systemer og lever dermed ikke op til de grundlæggende IT-sikkerhedsforanstaltninger som for eksempel opdatering af systemer. Ser man på virksomhedernes størrelse, er det i særlig grad de helt små virksomheder, der har flest sårbarheder.

Deloitte Cyber Risk-analyse: hackersimuleringer

I Deloitte Cyber Risks hackersimuleringer kigger man på virksomhedernes sårbarheder indenfor:

- Netværk: Denne kategori omhandler alt, der har med netværkstrafik og netværksenheder at gøre. Det vil sige alt, der transporterer og videreformidler informationer mellem netværkspunkter. Sårbarheder kan blandt andet være man in the middle-angreb ved hjælp af opsamling af netværkstrafik.
- Platform: Denne kategori omhandler netværksservices (HTTP(S), FTP, NTP, SMTP osv.) og konfiguration heraf (TLS/SSL, sikkerhedscertifikater m.m.).
- Applikation: Denne kategori omhandler selve (web)applikationen og/eller websitet. Det vil blandt andet sige fejlmeddelelser med sensitivt indhold, adgang til filer på applikationsserveren og funktionalitet, der kan udnyttes af uautoriserede personer.
- Database: Denne kategori omhandler den bagvedliggende database. Det kan for eksempel være sårbarheder som SQL injection, enumerering af databaseopslag og fingerprinting af databaseversion og type.

Ser man på tværs af virksomhederne, har 57 procent af virksomhederne haft yderst kritiske sårbarheder. Ser man på sårbarhedstyper, har de testede virksomheder forholdsvis flest kritiske og yderst kritiske sårbarheder[8] relateret til netværk og database. Dernæst er der relativt flest kritiske og yderst kritiske sårbarheder relateret til applikationer, og til sidst er der forholdsvis færrest kritiske og yderst kritiske sårbarheder relateret til platform.

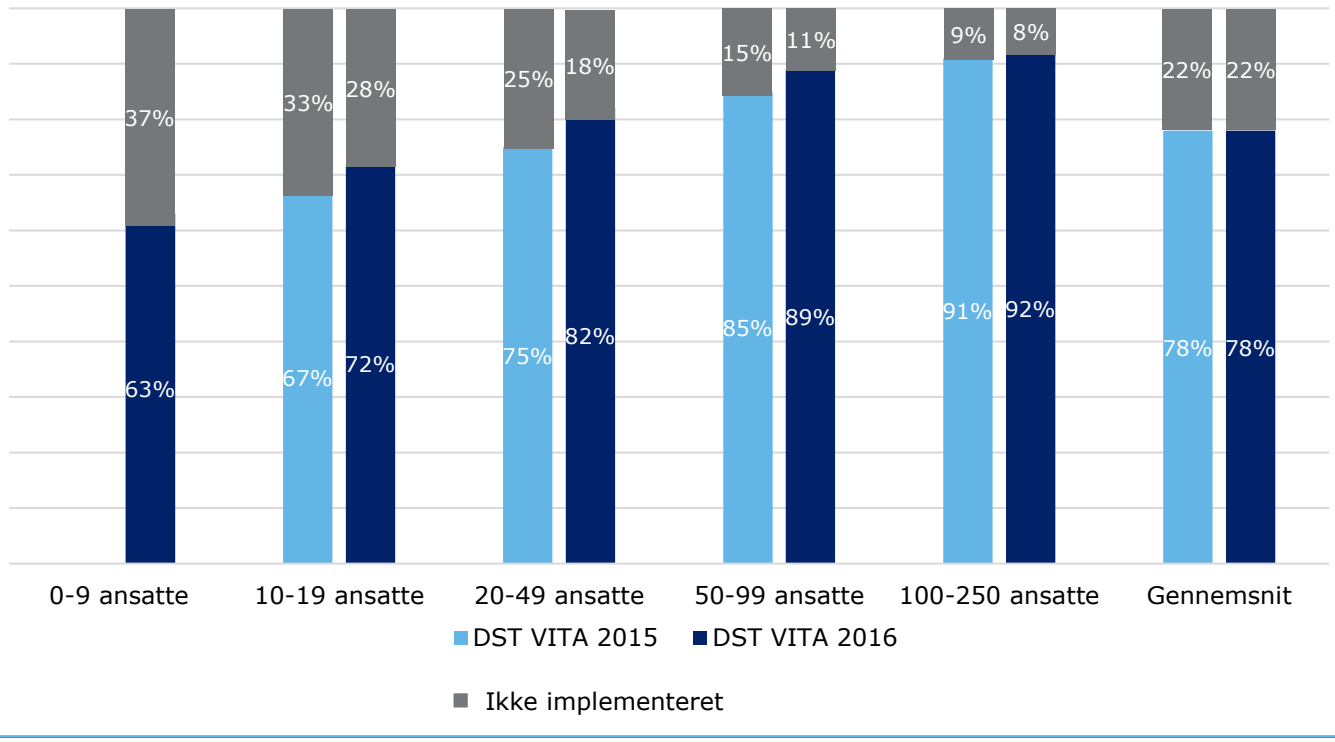
Når man ser på tværs af alle sårbarheder, ses der en tendens til, at mindre virksomheder i højere grad har kritiske og yderst kritiske sårbarheder. Virksomheder med 20-49 ansatte har i deres seneste scanning i gennemsnit haft 11 sårbarheder, mens tallet kun er 3 for virksomheder med 50-99 ansatte, og 2 for virksomheder med 100-199 ansatte.

I DST VITA-undersøgelsen fra henholdsvis 2015 og 2016 afdækkes det, om virksomhederne har implementeret grundlæggende IT-sikkerhedsforanstaltninger (defineret som følgende fire tiltag: firewall, antivirus, backup og databrugerrettigheder) i deres virksomheder. Her svarer 78 procent i både 2015- og 2016-undersøgelsen ja til, at de har implementeret grundlæggende IT-sikkerhedsforanstaltninger. Altså har cirka 22 procent ifølge DST VITA *ikke* implementeret de grundlæggende IT-sikkerhedsforanstaltninger. I denne sammenhæng skal man tage i betragtning, at man i DST VITA ikke skelner mellem, om man har implementeret alle eller enkelte tiltag. De 78 procent, der dermed svarer, at de har implementeret grundlæggende tiltag, vil sandsynligvis ikke have implementeret alle tiltag. Som det fremgår af Figur 12, er der dog sket en stigning i antallet af virksomheder, der har implementeret grundlæggende foranstaltninger, hvilket er positivt. Dette tyder på, at opmærksomheden om IT-sikkerhedstiltag er steget. I 2016 har man dog også inkluderet virksomheder med 0-9 ansatte, og da der er færre virksomheder i denne gruppe, der har implementeret grundlæggende IT-sikkerhedsforanstaltninger, stiger det samlede gennemsnit ikke.

I samme undersøgelse har kun cirka 30 procent implementeret avancerede foranstaltninger (defineret som følgende tiltag: gennemgang af logs, penetrationstest, beredskab og kontrol af sikkerhedstiltag).

[8] Sårbarheder med en CVSS-score (Common Vulnerability Scoring System) fra 6,0 og opefter.

Figur 12. Andel SMV'er, der har implementeret grundlæggende foranstaltninger



Kilde: DST VITA 2015 og 2016
Note: Grundlæggende foranstaltninger er for eksempel antivirusprogram, firewall, backup og databrugerrettigheder.

Tal fra både Deloitte Cyber Risk og DST VITA viser altså et lignende billede af SMV'ernes IT-sikkerhedsniveau som indeværende undersøgelse og viser ligeledes, at de mindre virksomheder har forholdsvis lavere IT-sikkerhedsniveau, hvilket bekræftes i det følgende.

Der er en række faktorer, der er medvirkende til, at over halvdelen af SMV'erne har et lavt IT-sikkerhedsniveau. I relation til de tre parametre, der udgør en virksomheds IT-sikkerhedsniveau, er der nogle centrale resultater, der er relevante at fremhæve.

Medarbejdere og ledelse:
- Mange danske SMV'er har ikke en formaliseret tilgang til IT-sikkerhed vedrørende medarbejdere, da de primært bruger mundtlig kommunikation til at gøre medarbejderne bevidste om IT-sikkerhed fremfor at bruge formaliserede tiltag som at træne medarbejderne i IT-sikkerhed og måle deres bevidsthed om samme.
- Det er i særlig grad de mindre virksomheder, der ikke har en formaliseret indsats rettet mod medarbejderne.
- I 83 procent af de danske SMV'er har ledelsen til en vis grad, i nogen grad eller i høj grad taget stilling til, hvordan IT-sikkerhed og databeskyttelse håndteres, og det fremgår, at graden af ledelsens stillingtagen er stærkt relateret til virksomhedens IT-sikkerhedsniveau.

IT-sikkerhedsforanstaltninger:
- En fjerdedel af de danske SMV'er har ikke implementeret essentielle IT-sikkerhedsforanstaltninger, der omfatter backupprocedurer og systematiske opdateringer af systemer og programmer.
- Der er generelt stor variation i danske SMV'ers niveau af IT-sikkerhedsforanstaltninger, hvilket man ser ved, at en forholdsvis stor del af de danske SMV'er har implementeret avancerede IT-sikkerhedstiltag, mens der også er en anseelig gruppe, der ikke har implementeret dette.

Fysisk adgangskontrol:
- Kun 60 procent af de danske SMV'er sikrer fysisk adgangskontrol vedrørende deres kritiske information.
- Om en virksomhed har fysisk adgangsstyring er i høj grad relateret til virksomhedens størrelse

Ovenstående gennemgås i detaljer i de efterfølgende afsnit.

Medarbejdere og ledelse

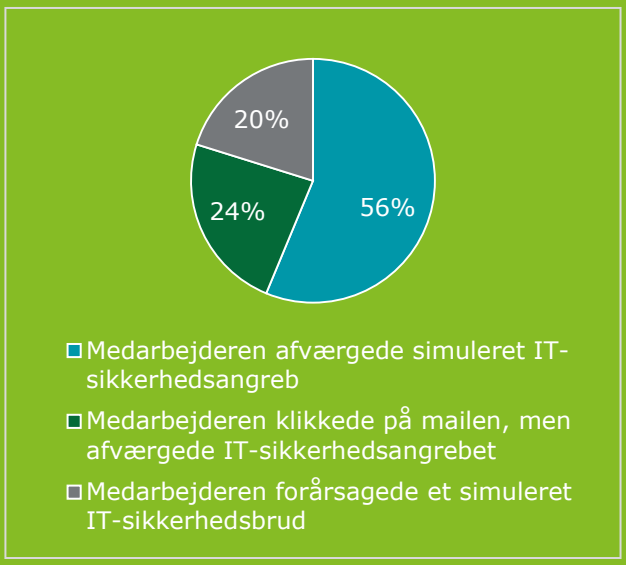
IT-sikkerhed relateret til medarbejderne vedrører i høj grad, hvordan IT-sikkerhed kommunikeres til medarbejderne, og i hvilket omfang medarbejderne er bevidste om IT-sikkerhedstrusler. Medarbejderne er en afgørende faktor indenfor IT-sikkerhed, da de kan være med til at forhindre et IT-sikkerhedsbrud ved at identificere et angreb, for eksempel en phishingmail. Derudover kan konsekvenserne ved et IT-sikkerhedsbrud mindskes, hvis medarbejderne identificerer det hurtigt og giver besked, for eksempel til den IT-ansvarlige. Resultater fra indeværende undersøgelse viser, at ved 39 procent af de IT-sikkerhedsbrud, som SMV'erne oplever, er det medarbejderne, der opdager det. Samtidig kan medarbejderne utilsigtet forårsage et IT-sikkerhedsbrud, hvis de ukritisk klikker på et link eller downloader indhold fra en phishingmail.

Det er derfor vigtigt at sikre, at medarbejderne har den nødvendige viden og de nødvendige kompetencer, så de aktivt kan deltage i at sikre et højt IT-sikkerhedsniveau.

Deloitte Cyber Risk-analyse: Virksomhedernes IT-sikkerhed afhænger af den enkelte medarbejder

Deloitte Cyber Risk har siden maj 2016 testet 40 virksomheder og myndigheder i medarbejdernes evne til at opfange phishingmails. Deloitte Cyber Risk sendte på foranledning af en anden afsender mails ud til virksomhedens ansatte, hvor der stod, at de ansatte skulle klikke på et link for at udfylde oplysninger. Mailene var falske og blev sendt med det formål at teste, om Deloitte Cyber Risk kunne franarre de ansatte hemmelige oplysninger, for eksempel deres password. I denne sammenhæng var det naturligvis som led i en test af medarbejdernes opmærksomhed på IT-sikkerhedsangreb og ikke et faktisk IT-sikkerhedsangreb.

Deloitte Cyber Risks undersøgelse viste, at samtlige testede virksomheder havde lidt et IT-sikkerhedsbrud, hvis det havde været en ægte phishingmail. Det vil sige, at en medarbejder både klikkede på linket i den falske mail og efterfølgende indtastede information eller downloadede en fil fra hjemmesiden, som man lander på efter at have klikket på linket. Ud af de samlede 16.713 mails, der blev sendt til virksomhederne, klikkede 3.938 på linket i mailen, hvoraf 3.372 var succesfulde, således der ville have været et IT-sikkerhedsbrud, som det er illustreret i figur 13 til højre. Undersøgelsen viser dermed, at omkring 44 procent af alle testede medarbejdere valgte at klikke på linket i phishingmailen, og at samlet set ville 20 procent af de testede personer have forårsaget et IT-sikkerhedsbrud, hvis der ikke blot havde været tale om en test.



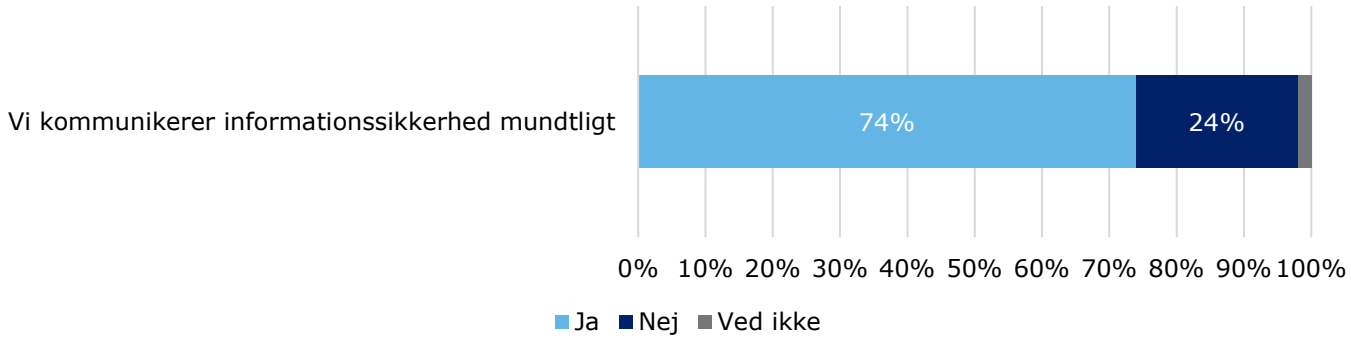
Figur 13. Andel udsendte mails, der resulterede i henholdsvis klik og brud

Den samme undersøgelse viser ligeledes, at mindre virksomheder (virksomheder med mindre end 250 ansatte) er mere udsatte end større virksomheder (virksomheder med mere end 250 ansatte). Dette ses blandt andet i denne undersøgelse ved, at en medarbejder i gennemsnit klikker på det tilsendte link i 44 procent af de udsendte mails til SMV'erne sammenlignet med 37 procent for de større virksomheder. Den andel, der havde lidt et IT-sikkerhedsbrud som følge af at klikke på linket og efterfølgende indtaste information på eller downloade filen fra hjemmesiden, er ligeledes højere for SMV'erne (20 procent af de udsendte mails til SMV'erne mod 16 procent for de større virksomheder).

4.2 Majoriteten af danske SMV'er har ikke en formaliseret tilgang til IT-sikkerhed vedrørende medarbejdere

Virksomhederne kan øge IT-sikkerheden på medarbejderniveau ved at øge medarbejdernes fokus på IT-sikkerhed gennem øget kommunikation. Her er mundtlig kommunikation et værdifuldt værktøj til at kommunikere om IT-sikkerhed.

Figur 14. Andel SMV'er, der kommunikerer informationssikkerhed mundtligt

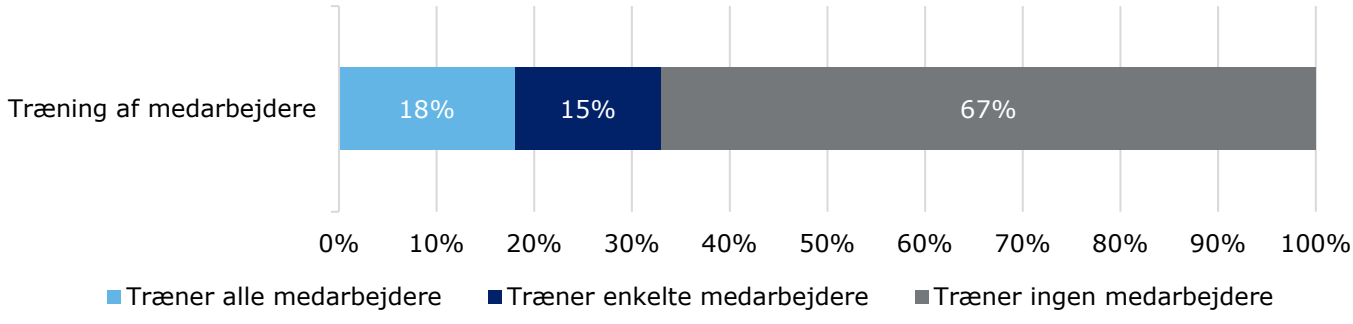


Kilde: Wilke for Monitor Deloitte

Som det fremgår af Figur 14, kommunikerer 74 procent af de danske SMV'er deres informationssikkerhed mundtligt. Den mundtlige kommunikation er en ikke-formaliseret måde at øge medarbejdernes viden om informationssikkerhed på, og en stor del af virksomhederne anvender denne tilgang.

Udover mundtlig kommunikation kan virksomhederne også anvende mere formaliserede tiltag i relation til IT-sikkerhed gennem formaliseret uddannelse eller træning i IT-sikkerhed. Dette benytter cirka en tredjedel af de danske SMV'er sig af, som det fremgår af Figur 15. Dette fordeles således, at 18 procent træner eller uddanner alle medarbejdere, mens 15 procent kun træner eller uddanner enkelte medarbejdere.

Figur 15. Andel SMV'er, der uddanner eller træner deres medarbejdere i IT-sikkerhed



Kilde: Wilke for Monitor Deloitte

Det er således hele 67 procent af de danske SMV'er, der ikke underviser eller træner deres medarbejdere i IT-sikkerhed, som det ses i Figur 15. Virksomheden AB Hjem er en af de virksomheder, der har valgt at øge indsatsen på dette område, som det ses af Case 1.[9]

[9] Ni casevirksomheder ønskede at være anonyme, hvorfor der er brugt aliasser ved disse virksomheder.

AB Hjem om formel træning af medarbejderne

Navn | AB Hjem

Branche | Fast ejendom

Størrelse | 160 medarbejdere

IT-sikkerhedsniveau | Middel

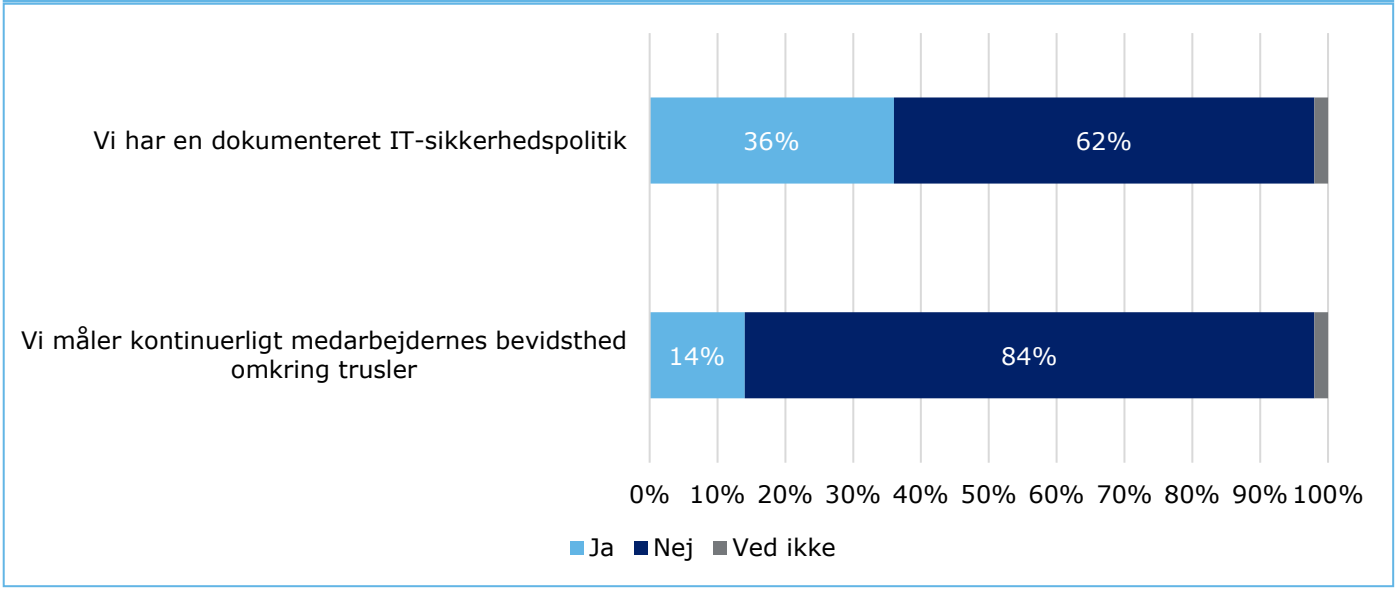
Risikoprofil | Middel

AB Hjem er en udlejningsvirksomhed, der udlejer til private.

AB Hjem har tidligere kun i begrænset omfang arbejdet med IT-sikkerhed relateret til medarbejderne, men det er noget, man ønsker at arbejde mere med fremadrettet. Virksomheden oplever, at medarbejderne har meget lidt fokus på IT-sikkerhed, og at medarbejderne ikke tænker over eksempelvis styrken af deres passwords. Da virksomheden ser, at den vil blive påvirket af persondataforordningen i fremtiden, ønsker den at øge fokus på IT-sikkerhed. Derfor planlægger man blandt andet at køre et uddannelses- og træningsprogram for at skabe forståelse af og opmærksomhed om IT-sikkerhed, og man håber, det kan være med til at forankre IT-sikkerhed i virksomhedskulturen.

Case 1. AB Hjem om formel træning af medarbejderne

Figur 16. Andel SMV'er, der har en dokumenteret IT-sikkerhedspolitik, og som måler på medarbejdernes bevidsthed



Kilde: Wilke for Monitor Deloitte

Ses der på andre formaliserede IT-sikkerhedstiltag målrettet medarbejderne, har få SMV'er implementeret disse. Af Figur 16 fremgår det, hvor mange af SMV'erne der har iværksat mere formaliserede IT-sikkerhedstiltag relateret til medarbejderne såsom en dokumenteret IT-sikkerhedspolitik og måling af medarbejdernes bevidsthed om trusler. Det er tydeligt, at en langt mindre del har en formaliseret tilgang til IT-sikkerhed, og kun en lille del af virksomhederne måler på medarbejdernes bevidsthed om IT-sikkerhedstrusler. Dette bekræftes også af DST VITA fra 2016, hvoraf det fremgår, at 42 procent har retningslinjer vedrørende IT-sikkerhed til medarbejderne, hvilket også understreger, at virksomhederne i mindre grad arbejder med formaliserede tiltag målrettet medarbejderne. Årsagen til den lave grad af anvendelse af formaliserede tiltag kan være, at virksomhederne starter deres arbejde med IT-sikkerhed med den mundtlige kommunikation, hvorefter de bygger mere formaliserede tiltag på.

Det har stor betydning for virksomhedens samlede IT-sikkerhed, om den har formaliseret tiltagene på området. 92 procent af de virksomheder, der har et højt IT-sikkerhedsniveau, har en dokumenteret IT-sikkerhedspolitik, og 49 procent måler medarbejdernes bevidsthed om IT-sikkerhedstrusler. For virksomheder med et lavt IT-

sikkerhedsniveau har kun 15 procent en dokumenteret IT-sikkerhedspolitik, og kun 5 procent måler på medarbejdernes bevidsthed om IT-sikkerhedstrusler.

Virksomheder med en høj risikoprofil anvender mere formaliserede IT-sikkerhedstiltag. 56 procent af de virksomheder, der har en høj risikoprofil, har en dokumenteret IT-sikkerhedspolitik, og 26 procent måler medarbejdernes bevidsthed om IT-sikkerhedstrusler. Kun 20 procent af de virksomheder, der har en lav risikoprofil, har en dokumenteret IT-sikkerhedspolitik, og kun 7 procent måler medarbejdernes bevidsthed om IT-sikkerhedstrusler.

10 af de 14 virksomheder i caseinterviewene bruger den uformelle kommunikation som en katalysator til at forankre IT-sikkerhed i virksomhedskulturen. Dette bekræfter, at de ikke-formaliserede tiltag relateret til medarbejderne er et af de ofte anvendte redskaber til at fremme IT-sikkerhed blandt medarbejderne. Det kan skyldes, at den mundtlige kommunikation er det nemmeste at implementere, og at man derfor ofte starter sit arbejde her. I takt med at virksomhedens IT-sikkerhed modnes, bygger man mere formaliserede tiltag på for at øge IT-sikkerheden relateret til medarbejderne. TP Aerospace er et eksempel på en virksomhed, hvor man startede med at have fokus på kommunikationen til medarbejderne for derigennem at forankre en forståelse af IT-sikkerhed i virksomhedskulturen. Dette fremgår af Case 2.

TP Aerospaces rejse fra grundlæggende til avanceret IT-sikkerhed og brug af uformel kommunikation

Navn | TP Aerospace

Branche | Handel

Størrelse | 220 medarbejdere

It-sikkerhedsniveau | Middel

Risikoprofil | Lav

TP Aerospace sælger flyhjul og -bremser til mindre fly- og fragtselskaber og henvender sig til internationale markeder.

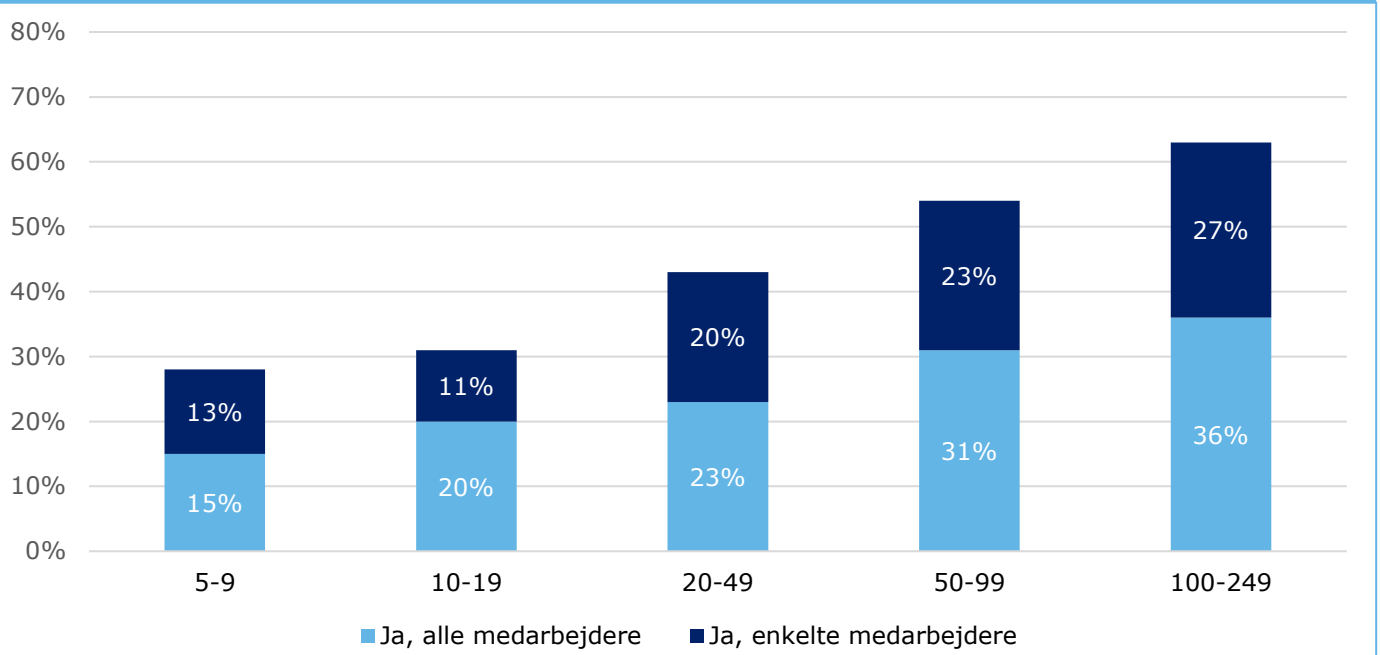
TP Aerospace er siden virksomhedens begyndelse vokset meget i både omsætning og medarbejdere, og IT-sikkerhed har kun været en lille del af forretningen. I 2016 vurderede ejerne, at det var nødvendigt med en IT-ansvarlig, da de ikke længere selv kunne varetage deres IT-drift. Som et led i dette startede de derfor helt fra bunden med at opbygge deres IT-sikkerhed, da virksomheden ansatte en IT-ansvarlig. I arbejdet med IT-sikkerhed var der indledningsvist fokus på at kommunikere til medarbejderne, hvorfor IT-sikkerhed var nødvendigt, og hvad det betød for dem i deres daglige arbejde. Den IT-ansvarlige oplevede, at medarbejdernes begrænsede viden om IT-sikkerhed var en barriere, og det stod klart, at det krævede en kulturændring, og man startede derfor indsatsen med den uformelle kommunikation. Da man var nået langt med kommunikation, ønskede virksomheden at lægge et lag mere på den indsats, der var målrettet medarbejderne, hvorfor man gennemførte et uddannelses- og træningsprogram målrettet medarbejderne. Samme program blev brugt til at måle medarbejdernes bevidsthed om IT-

Case 2. TP Aerospace

4.3 Små virksomheder arbejder ikke formaliseret med IT-sikkerhed relateret til medarbejderne

Case 2 om TP Aerospace indikerer, at jo længere virksomheden har arbejdet med IT-sikkerhed, jo flere formaliserede tiltag implementerer virksomheden. Det er også en indikation af, at jo større virksomheden er, jo længere vil den have arbejdet med IT-sikkerhed og derfor have flere formaliserede tiltag.

Figur 17. Andel SMV'er, der uddanner eller træner deres medarbejdere i IT-sikkerhed på tværs af virksomhedsstørrelse



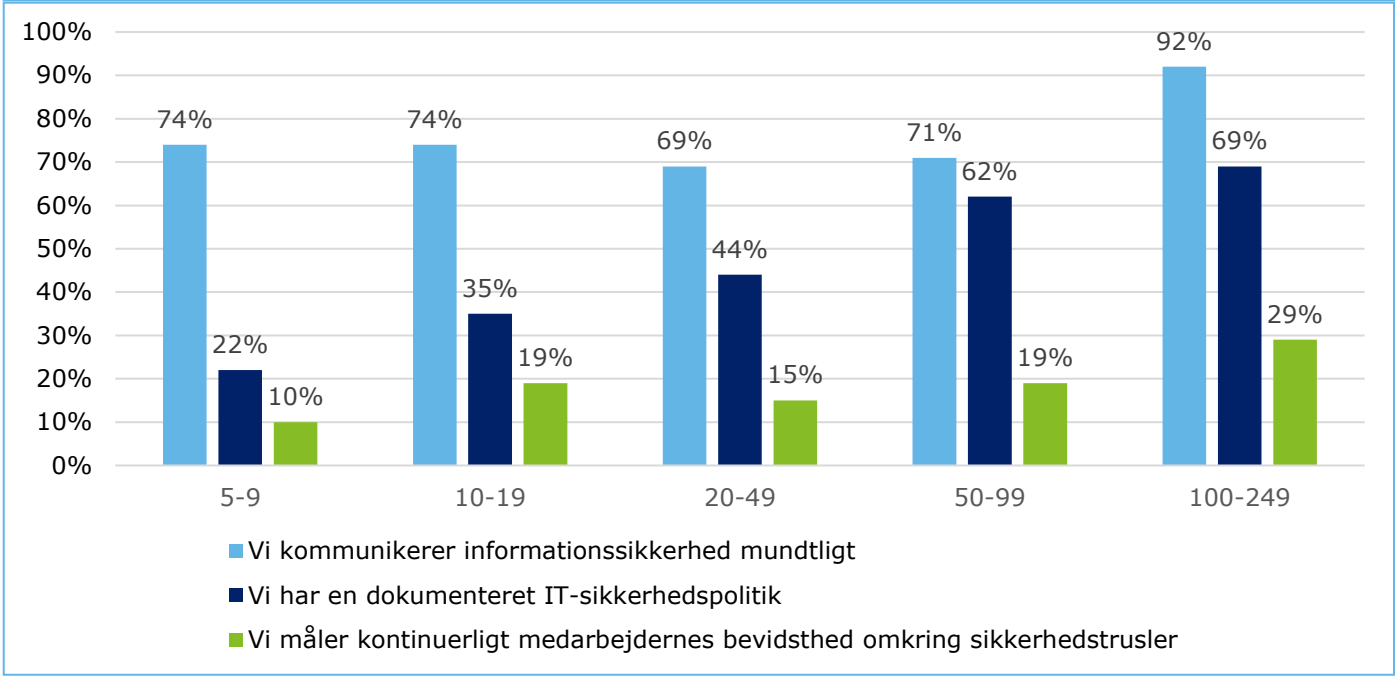
Kilde: Wilke for Monitor Deloitte

Figur 17 viser andelen af virksomheder, der træner deres medarbejdere i IT-sikkerhed i forhold til virksomhedens størrelse. På tværs af virksomhedsstørrelse ses der en klar relation mellem virksomhedens størrelse, og om virksomheden træner sine medarbejdere i IT-sikkerhed. Der er flere større virksomheder, der uddanner eller træner deres medarbejdere, hvilket netop indikerer, at større virksomheder er mere modne og dermed arbejder mere formaliseret med IT-sikkerhed. 28 procent af de virksomheder, der har 5-9 ansatte, uddanner eller træner alle eller enkelte medarbejdere, mens dette tal er 63 procent for virksomheder med 100-249 ansatte.

Der er forskel på, om man træner alle eller enkelte medarbejdere i IT-sikkerhed. Dette kan skyldes, at der internt er et forskelligt behov, afhængigt af hvor mange medarbejdere der bruger IT, og hvor mange der har adgang til kritiske data og systemer. Det bør dog medtages, at grundlæggende viden om IT-sikkerhed er relevant for alle medarbejdere, idet hackere for eksempel ved brug af phishingmails kan rette angreb mod langt de fleste medarbejdere.

Som beskrevet ovenfor, vil mindre virksomheder oftere være mere umodne i deres IT-sikkerhed, og deres fokus er derfor primært på de ikke-formaliserede tiltag, før man implementerer formaliserede tiltag i relation til IT-sikkerhed. Dette bekræftes også af Figur 18. Det kan dog også være et ressourcespørgsmål, da ikke-formaliserede tiltag er billigere, og det er derfor lettere for mindre virksomheder at anvende disse tiltag.

Figur 18. Andel SMV'er, der bruger forskellige IT-sikkerhedstiltag målrettet medarbejderne på tværs af virksomhederne



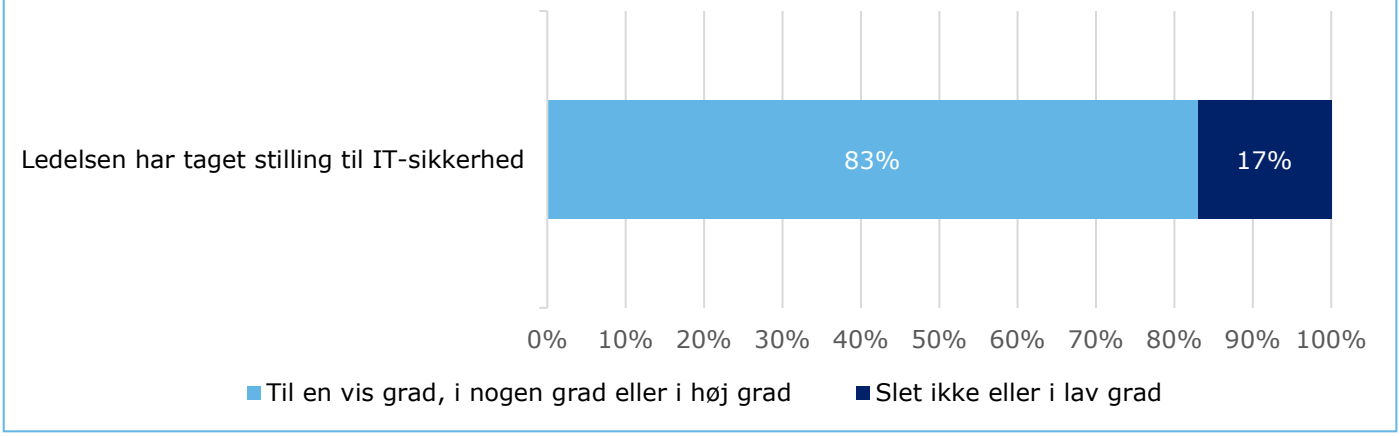
Kilde: Wilke for Monitor Deloitte

Figur 18 viser, hvor stor en andel af virksomhederne der har implementeret IT-sikkerhedsrelaterede tiltag i forhold til medarbejderne på tværs af virksomhedernes størrelse. Cirka en lige stor andel på tværs af virksomhedsstørrelse kommunikerer informationssikkerhed mundtligt. Størstedelen af virksomhederne bruger de ikke-formaliserede tiltag til IT-sikkerhed i forhold til medarbejderne. Der ses en stigning i den andel, der har en dokumenteret IT-sikkerhedspolitik, i takt med at virksomhederne bliver større. Dette understreger, at mindre virksomheder har en lavere grad af formaliserede IT-sikkerhedstiltag, men i stedet implementerer ikke-formaliserede IT-sikkerhedstiltag. I DST VITA fra 2016 er dette billede det samme, idet det fremgår, at 62 procent af de virksomheder, der har 100-249 ansatte, har retningslinjer vedrørende IT-sikkerhed til medarbejderne, mens det kun gælder 34 procent af virksomhederne med 10-19 ansatte.

4.4 Ledelsens manglende stillingtagen til IT-sikkerhed er en begrænsning for IT-sikkerhedsniveauet

Ligesom medarbejderne spiller ledelsen også en stor rolle i forhold til IT-sikkerhed, da det er dem, der allokerer ressourcer til arbejdet med IT-sikkerhed, og de har samtidig en vigtig indvirkning på virksomhedskulturen. Det er derfor væsentligt, at de forholder sig til IT-sikkerhed.

Figur 19. Andel SMV'er, hvor ledelsen har taget stilling til IT-sikkerhed

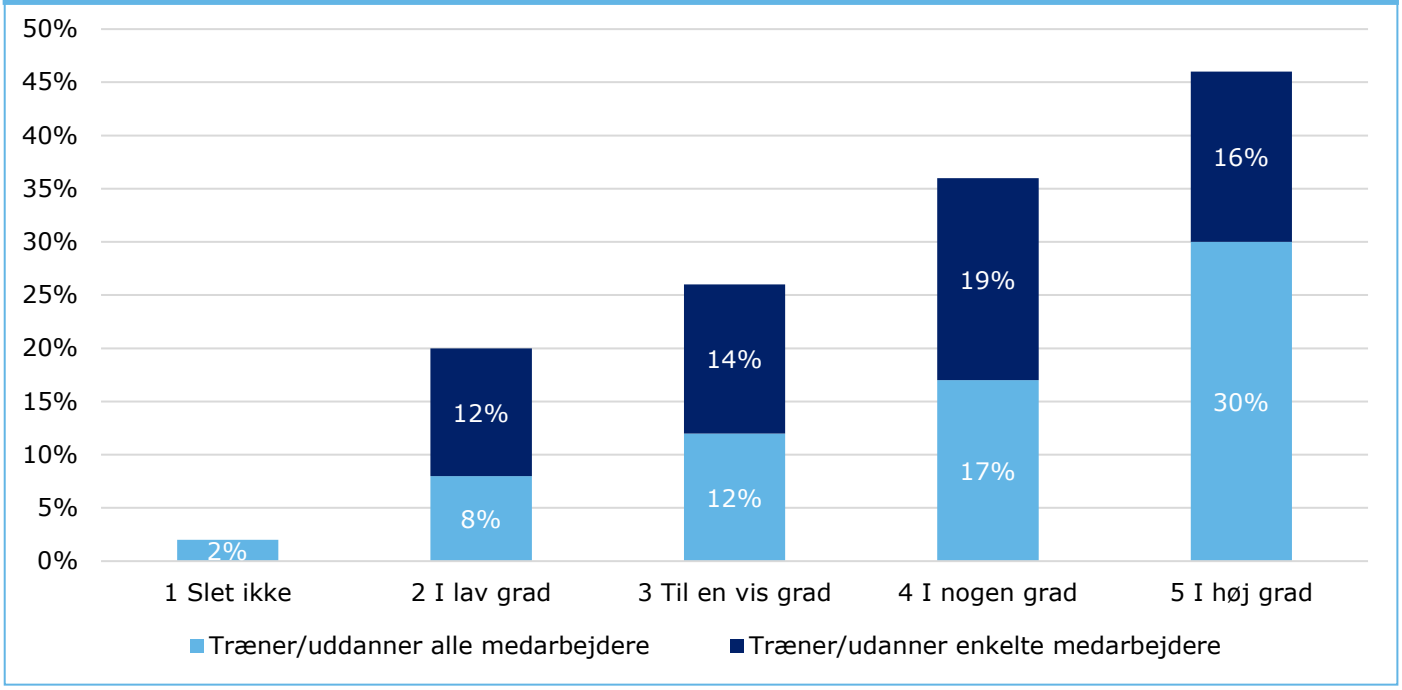


Kilde: Wilke for Monitor Deloitte

I 83 procent af virksomhederne har ledelsen til en vis grad, i nogen grad eller i høj grad taget stilling til IT-sikkerhed, og det er således størstedelen, som det fremgår af Figur 19. Dette viser, at IT-sikkerhed i høj grad er kommet ind på radaren i dansk erhvervsliv, men der er stadig behov for at få de sidste med.

Sammenhængen mellem, om ledelsen har taget stilling til IT-sikkerhed, og om virksomheden træner sine medarbejdere, understreger betydningen af ledelsens stillingtagen for en virksomheds IT-sikkerhed, som det er vist i Figur 20. Man kunne tro, at ledelsens stillingtagen også hang sammen med virksomhedens størrelse, men der er ikke en statistisk sammenhæng mellem disse to parametre.

Figur 20. Sammenhængen mellem ledelsens stillingtagen og træning/uddannelse af medarbejderne i IT-sikkerhed

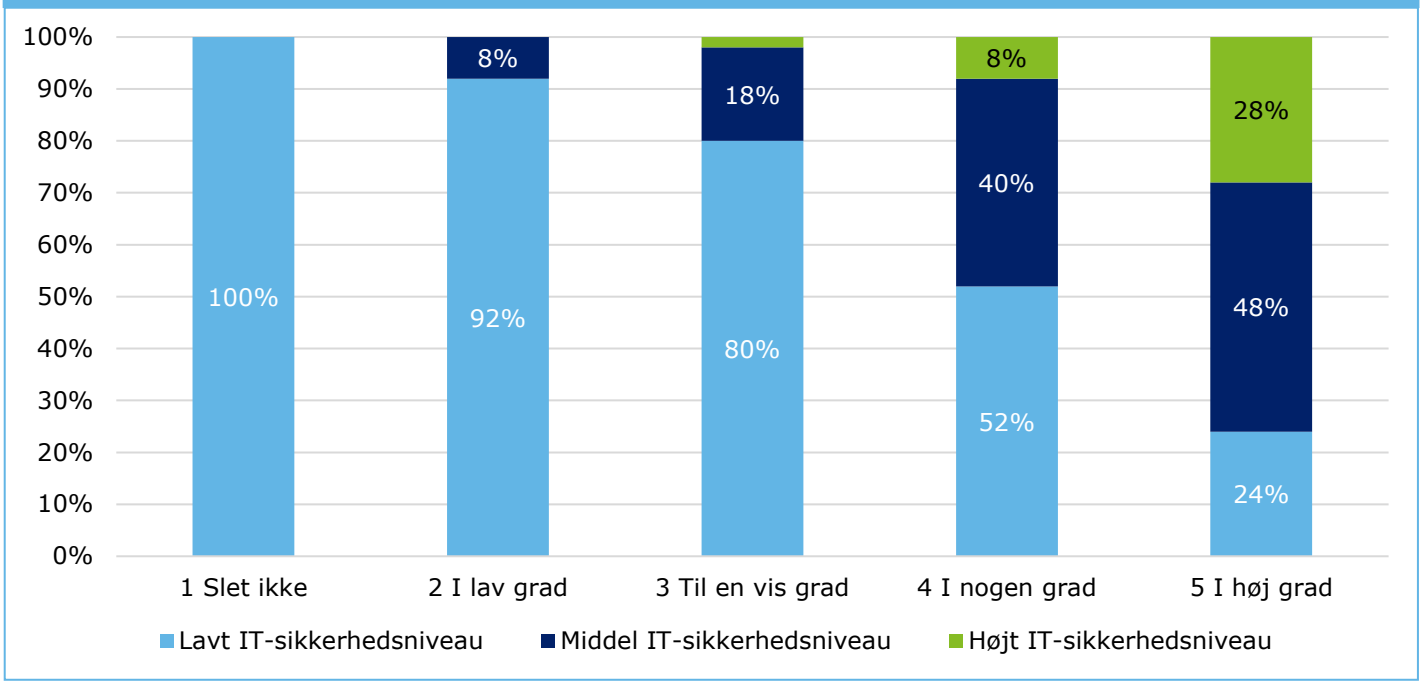


Kilde: Wilke for Monitor Deloitte og Monitor Deloitte-analyse

Som det fremgår af Figur 20, er der en klar tendens til, at i jo højere grad ledelsen har taget stilling til IT-sikkerhed, i jo højere grad træner virksomheden sine medarbejdere. Dette understreger vigtigheden af, at ledelsen involveres i IT-sikkerhed.

Ledelsens stillingtagen har også stor betydning for virksomhedens samlede IT-sikkerhedsniveau.

Figur 21. Sammenhængen mellem ledelsens stillingtagen og IT-sikkerhedsniveauet



Kilde: Wilke for Monitor Deloitte og Monitor Deloitte-analyse

I Figur 21 vises sammenhængen mellem, i hvilken grad ledelsen har taget stilling til IT-sikkerhed og virksomhedens IT-sikkerhedsniveau. Også her ses der en tendens til, at ledelsens stillingtagen har stor betydning og er stærkt relateret til virksomhedens IT-sikkerhedsniveau. Har ledelsen slet ikke taget stilling til IT-sikkerhed, har alle virksomhederne et lavt IT-sikkerhedsniveau. Denne andel falder, i takt med at ledelsen i højere grad har taget stilling til IT-sikkerhed, og man ser i særlig grad en udvikling fra svarene *3 Til en vis grad* til *5 I høj grad*. For virksomheder, hvor ledelsen i høj grad har taget stilling til IT-sikkerhed, har kun 24 procent af virksomhederne et lavt IT-sikkerhedsniveau, 48 procent har et middel IT-sikkerhedsniveau, mens 28 procent har et højt IT-sikkerhedsniveau.

Maskinhandler Indkøbsringen anerkendte også ledelsens indflydelse på IT-sikkerheden, og derfor gjorde de IT-ansvarlige en indsats for at sikre, at ledelsen ønskede en højere grad af IT-sikkerhed, som det fremgår af Case 3.

Maskinhandler Indkøbsringen om vigtigheden af at inddrage ledelsen i IT-sikkerhedsarbejdet

Navn | Maskinhandler Indkøbsringen

Branche | Handel

Størrelse | 65 medarbejdere

IT-sikkerhedsniveau | Middel

Risikoprofil | Middel

Virksomheden er et indkøbssamarbejde mellem danske maskinforretninger, der sælger maskiner til private og erhverv.

Hos Maskinhandler Indkøbsringen indså de IT-ansvarlige, at det var nødvendigt at øge virksomhedens IT-sikkerhed, da det nuværende niveau ikke var tilstrækkeligt for virksomhedens risikoprofil. Man vidste fra starten, at det var vigtigt at få ledelsen med ombord. Man så, at ledelsen var en vigtig faktor i arbejdet med IT-sikkerhed, da det var ledelsen, der skulle allokere de nødvendige ressourcer. De IT-ansvarlige forventede, at det ville blive svært at få ledelsens godkendelse af de nødvendige ressourcer, da ledelsen ikke vidste meget om IT-sikkerhed. De IT-ansvarlige valgte derfor at inddrage ledelsen tidligt i forløbet, så man kunne få de nødvendige midler til arbejdet. Dette gjorde man blandt andet ved at få en ekstern aktør til at udarbejde en sikkerhedsanalyse, og man brugte så denne i kommunikationen til ledelsen. Dette betød, at ledelsen fik mere forståelse af vigtigheden af IT-sikkerhed og accepterede tiltagene og endda valgte at engagere sig i arbejdet.

Case 3. Maskinhandler Indkøbsringen

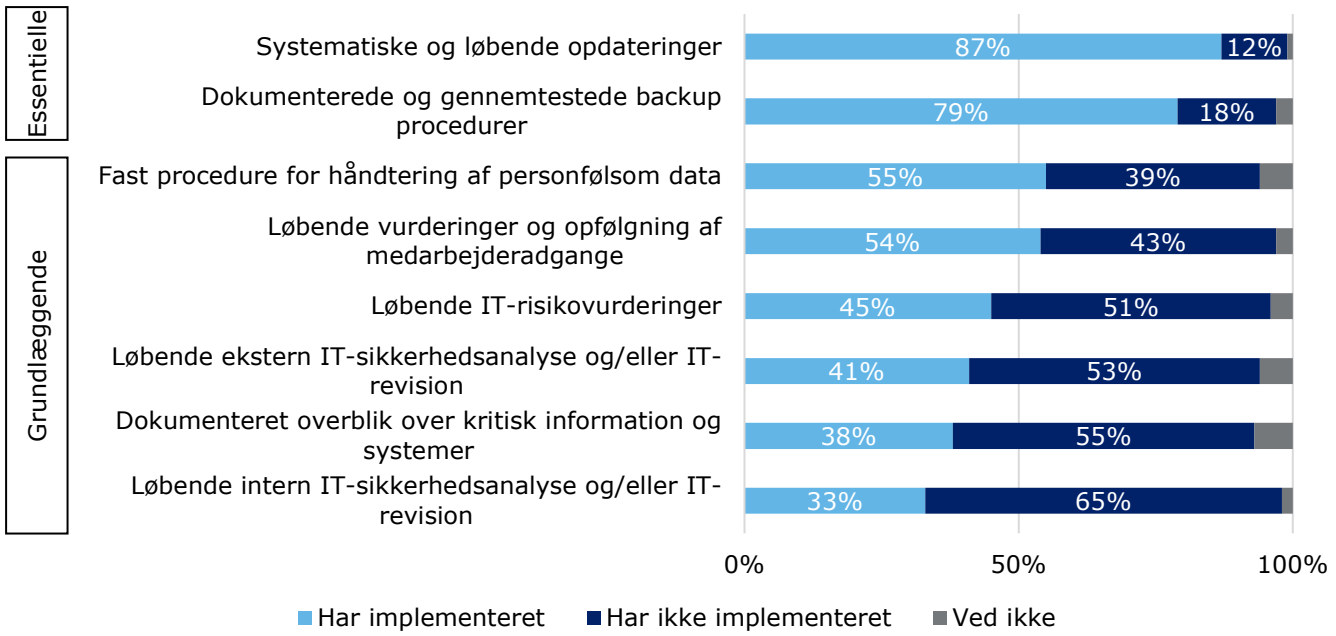
IT-sikkerhedsforanstaltninger

En virksomhed kan implementere en række IT-sikkerhedsforanstaltninger for at øge IT-sikkerheden og for at beskytte virksomheden mod eventuelle IT-sikkerhedsangreb. Man kan tale om to IT-sikkerhedsforanstaltningsniveauer: grundlæggende og avanceret. Det vil i det følgende blive afdækket, i hvilket omfang danske SMV'er har implementeret IT-sikkerhedsforanstaltningerne inden for disse.

4.5 En fjerdedel af virksomhederne har ikke implementeret essentielle IT-sikkerhedsforanstaltninger

Under de grundlæggende IT-sikkerhedsforanstaltninger er der nogle helt essentielle foranstaltninger, der anses for at være nødvendige for enhver virksomhed, nemlig dokumenteret og gennemtestet backup og opdatering af systemer og programmer. Disse IT-sikkerhedsforanstaltninger anses for at være essentielle, da de udover at være relevante for at kunne afværge mange IT-sikkerhedsangrebstyper også er relativt simple at indføre for virksomheden. Derudover er der en lang række andre grundlæggende IT-sikkerhedsforanstaltninger, som det fremgår af Figur 22.

Figur 22. Andel SMV'er, der har implementeret essentielle og grundlæggende IT-sikkerhedsforanstaltninger



Kilde: Wilke for Monitor Deloitte

Som det fremgår af Figur 22, har 88 procent af SMV'erne implementeret systematiske og løbende opdateringer, mens 82 procent har implementeret dokumenterede og gennemtestede backupprocedurer. Ser man på tværs af disse to IT-sikkerhedsforanstaltninger, har 74 procent af virksomhederne implementeret begge disse essentielle IT-sikkerhedsforanstaltninger. Der er således cirka en fjerdedel, svarende til 23 procent, der ikke har implementeret begge disse essentielle IT-sikkerhedsforanstaltninger (3 procent har svaret *ved ikke*). Ud af de 23 procent har cirka en fjerdedel, svarende til 6 procent af de danske SMV'er, ikke implementeret nogen af de essentielle tiltag. Et lignende mønster finder man i DST VITA fra 2016, hvoraf det fremgår, at 78 procent af SMV'erne har implementeret IT-sikkerhedstiltag som antivirusprogram, firewall og backup, og det bekræfter dermed, at en relativt stor del af SMV'erne ikke har implementeret disse vigtige IT-sikkerhedsforanstaltninger.

Af Figur 22 fremgår det desuden, at en stor del af virksomhederne ikke har implementeret de resterende grundlæggende IT-sikkerhedstiltag. Det er i særlig grad IT-sikkerhedsanalyser og/eller IT-revision og et dokumenteret overblik over kritisk information og systemer, hvor implementeringsgraden er lav. Ser man på tværs af de resterende grundlæggende IT-sikkerhedstiltag, har kun gennemsnitligt 49 procent implementeret disse (heri indregnes, at man enten har implementeret intern eller ekstern IT-sikkerhedsanalyse og/eller IT-revision). Det er således flere end halvdelen, der ikke har implementeret de grundlæggende IT-sikkerhedstiltag. Ses der isoleret på IT-sikkerhedsanalyse og/eller IT-revision er det 45 procent, der hverken foretager dette internt eller eksternt, mens 19 procent foretager både intern og ekstern IT-sikkerhedsanalyse og/eller IT-revision. Dette understreger pointen om, at der er store forskelle på IT-sikkerhedsniveauet i danske SMV'er.

Årsagen til, at man som virksomhed ikke implementerer de essentielle IT-sikkerhedstiltag, kan være, at virksomhederne ikke har den nødvendige indsigt i behovet for disse tiltag, fordi man ikke har den fulde forståelse af risikoen for et IT-sikkerhedsangreb og de potentielle konsekvenser ved et IT-sikkerhedsbrud. Danmarks Naturfredningsforening havde ikke implementeret backup, da man for over 10 år siden oplevede et systemnedbrud. Det fremgår af Case 4, hvilke konsekvenser det fik for virksomheden.

Danmarks Naturfredningsforening om vigtigheden af essentiel IT-sikkerhed

Navn | Danmarks Naturfredningsforening

Branche | Offentlig forvaltning og forsvar

Størrelse | 70 medarbejdere

It-sikkerhedsniveau | Middel

Risikoprofil | Middel

Danmarks Naturfredningsforening er en forening, der arbejder for at bevare landskabet og naturen i Danmark.

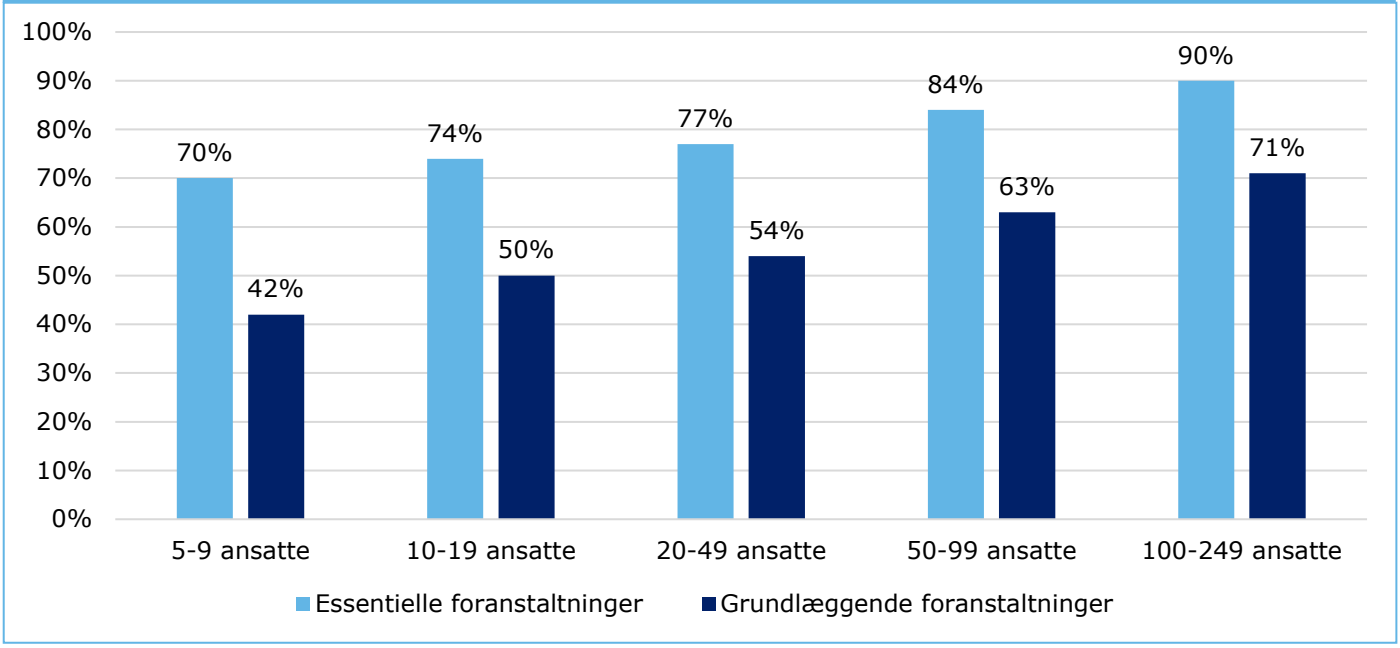
I Danmarks Naturfredningsforening havde man ikke implementeret de essentielle IT-sikkerhedsforanstaltninger, da man for over 10 år siden havde et systemnedbrud, hvor man mistede en del af sine medlemsdata. Da man ikke havde en systematisk backupprocedure for disse data, kunne data ikke genskabes, hvilket betød, at dataene var tabt. Da disse data var grundlaget for virksomheden, og den måde de tjente penge på, var det nødvendigt at få dataene tilbage. Løsningen på problemet blev at indsamle data fra forskellige filer på forskellige medarbejderes computere. De nøjagtige omkostninger i forbindelse med genskabelse af de krypterede data er vanskelige at estimere, men konsekvensen har kunnet mærkes.

Idet Danmarks Naturfredningsforening mærkede konsekvensen af ikke at have backup af deres data, har virksomheden siden implementeret en systematisk backupprocedure.

Case 4. Danmarks Naturfredningsforening

Den bagvedliggende årsag til, at en stor del af virksomhederne ikke har implementeret de resterende grundlæggende tiltag, kan være, at virksomhederne vurderer, at foranstaltningerne ikke er nødvendige. Det kan for eksempel være tilfældet, hvis man ikke foretager tilstrækkelig risikovurdering, eller hvis ledelsen ikke prioriterer de nødvendige ressourcer. Årsagen kan også være, at man ikke kender til disse IT-sikkerhedsforanstaltninger, fordi man ikke har tilstrækkelige IT-kompetencer internt i virksomheden til at vide, at disse foranstaltninger er centrale i virksomhedens forsvar mod IT-sikkerhedsangreb.

Figur 23. Andel SMV'er, der har implementeret grundlæggende IT-sikkerhedsforanstaltninger på tværs af virksomhedsstørrelse



Kilde: Wilke for Monitor Deloitte og Monitor Deloitte-analyse

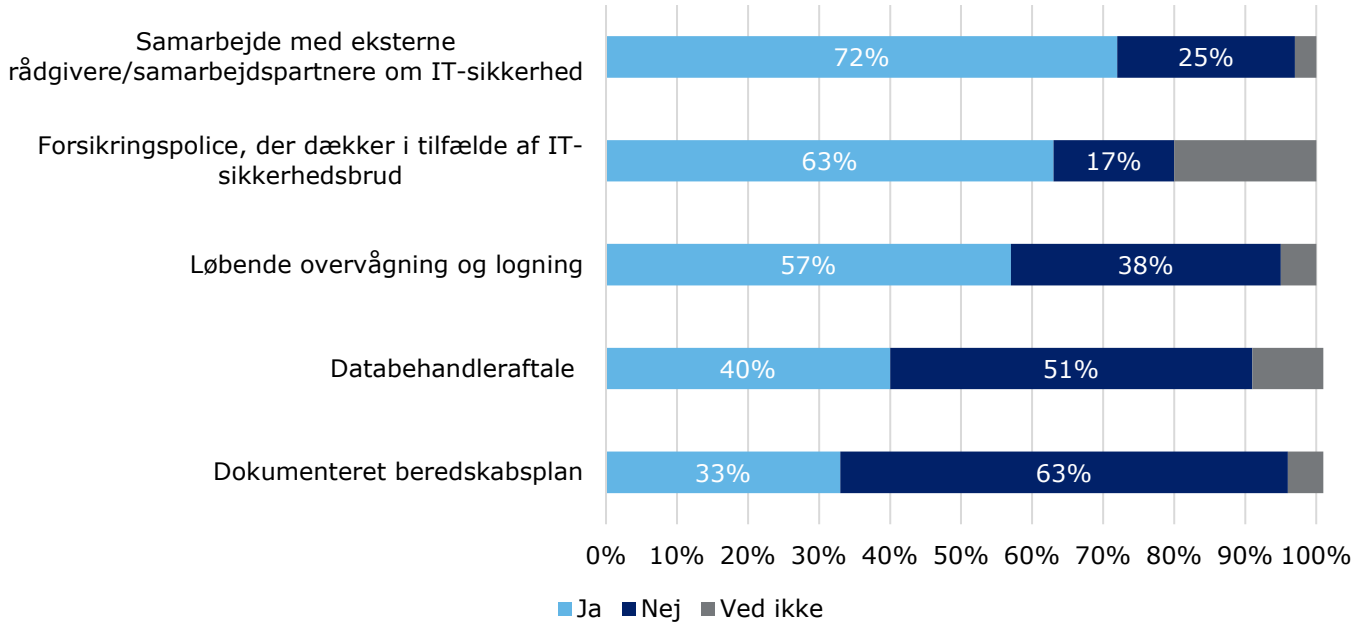
I Figur 23 er det vist på tværs af virksomhedsstørrelse, hvor stor en andel der har implementeret essentielle og grundlæggende IT-sikkerhedstiltag. Der ses en tendens til, at en større andel af de større virksomheder har implementeret de grundlæggende IT-sikkerhedstiltag sammenlignet med de helt små virksomheder. Der ses især en stor ændring i de grundlæggende foranstaltninger, der stiger fra 42 procent for virksomheder med 5-9 ansatte til 71 procent for virksomheder med 100-249 ansatte. Denne tendens understøttes af DST VITA fra 2016, hvoraf det fremgår, at 63 procent af de virksomheder, der har 0-9 ansatte, har implementeret grundlæggende IT-sikkerhedsforanstaltninger i 2016, mens dette tal er 92 procent for virksomheder med 100-249 ansatte i 2016.

Som ved brugen af ikke-formaliserede og formaliserede IT-sikkerhedstiltag relateret til medarbejderne kan dette skyldes, at man som virksomhed starter med at implementere de essentielle IT-sikkerhedsforanstaltninger for derefter at bygge ovenpå med de grundlæggende tiltag, efterhånden som virksomheden vokser, og IT-sikkerheden bliver mere moden.

4.6 En stor del af virksomhederne anvender avancerede IT-sikkerhedsforanstaltninger

Det højeste niveau for IT-sikkerhedsforanstaltninger er de avancerede IT-sikkerhedstiltag, der er særlig relevant for virksomheder med stor afhængighed til data og IT-systemer.

Figur 24. Andel SMV'er, der har implementeret avancerede IT-sikkerhedsforanstaltninger



Kilde: Wilke for Monitor Deloitte

Af Figur 24 fremgår det, hvor mange virksomheder der har implementeret avancerede IT-sikkerhedsforanstaltninger. 72 procent af virksomhederne samarbejder med eksterne rådgivere/samarbejdspartnere. Dette bekræftes også af caseinterviewene, hvor størstedelen nævner, at de bruger eksterne samarbejdspartnere, og at det i høj grad er fra disse, de får information om IT-sikkerhed. Givet at tiltagene vist i Figur 24 er til den mere avancerede side, er det interessant, at der ikke er væsentlig færre, der har implementeret disse end de grundlæggende tiltag, men at de ligger på cirka samme niveau. Af DST VITA for 2016 fremgår det, at 47 procent af virksomhederne har implementeret avancerede IT-sikkerhedstiltag, der omfatter gennemgang af logs, penetrationstest, beredskab og kontrol af sikkerhedstiltag, og gennemsnittet for Figur 24 er 48 procent (når man ser bort fra samarbejde med eksterne). Tallene fra DST VITA ligger derfor tæt med tallene fra indeværende undersøgelse. Det er dog ikke helt de samme parametre, der måles på, og tallene kan derfor ikke sammenlignes en til en.

63 procent af respondenterne svarer, at de har en forsikringspolice, der dækker i tilfælde af IT-sikkerhedsbrud. Dette tal virker meget højt, da denne type forsikring stadig er ny på markedet. Forsikringsselskabet Tryg har i november 2017 for eksempel kun solgt 400 forsikringer til SMV'er, hvilket svarer til cirka 5 procent af deres kundeportefølje i dette segment.[10] Det er derfor usikkert, om de 63 procent er retvisende. Dette bekræftes også af, at hele 20 procent ikke ved, om de har denne type forsikring, hvilket viser virksomhedernes usikkerhed om dette. Her er der potentielt en risiko for, at mange SMV'er tror, de er forsikret uden reelt at være det.

Fysisk adgangskontrol

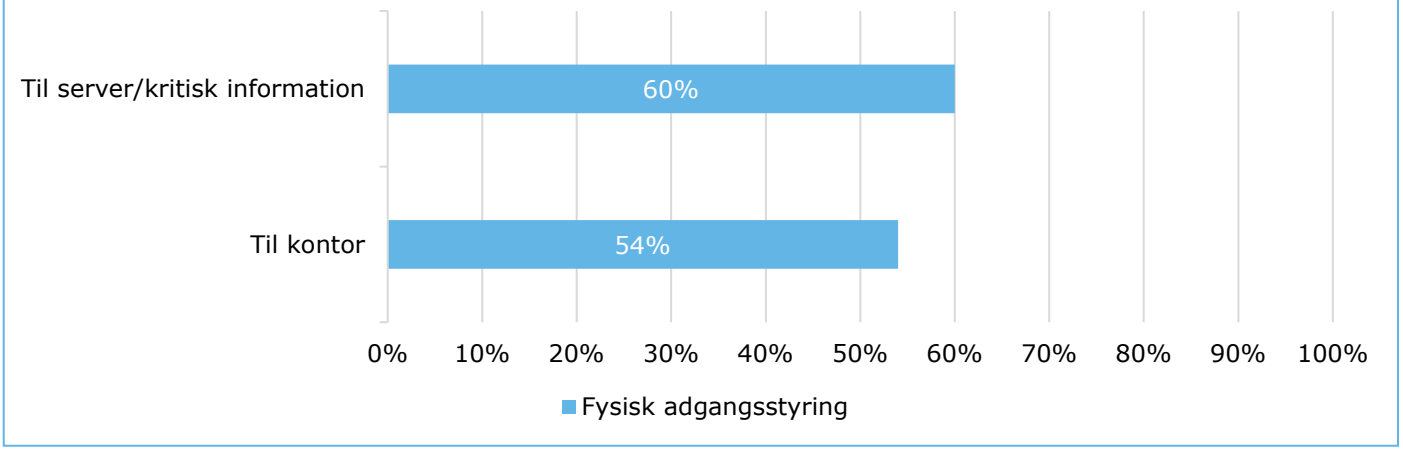
Fysisk adgangskontrol er et meget basalt IT-sikkerhedstiltag, idet man her sikrer, at det ikke er alle og enhver, der kan få adgang til ens servere, data, systemer og computere. Fysisk adgangskontrol betyder, at man har sikret adgang til kontor og/eller servere ved at have personlige nøglekort/chip, så man kan begrænse, hvem der kan tilgå kontoret og serverne, og logge, hvem der kommer ind og hvornår.

[10] http://itwatch.dk/ITNyt/Brancher/Sikkerhed/article10042390.ece

4.7 Kun 60 procent sikrer fysisk adgang til deres kritiske information

Når man ser på fysisk adgangskontrol, kan man både inddrage kontrol i forhold til adgang til kontoret og i forhold til adgang til virksomhedens kritiske information/servere.

Figur 25. Andel SMV'er, der har påbegyndt fysisk adgangsstyring til kontor og kritisk information

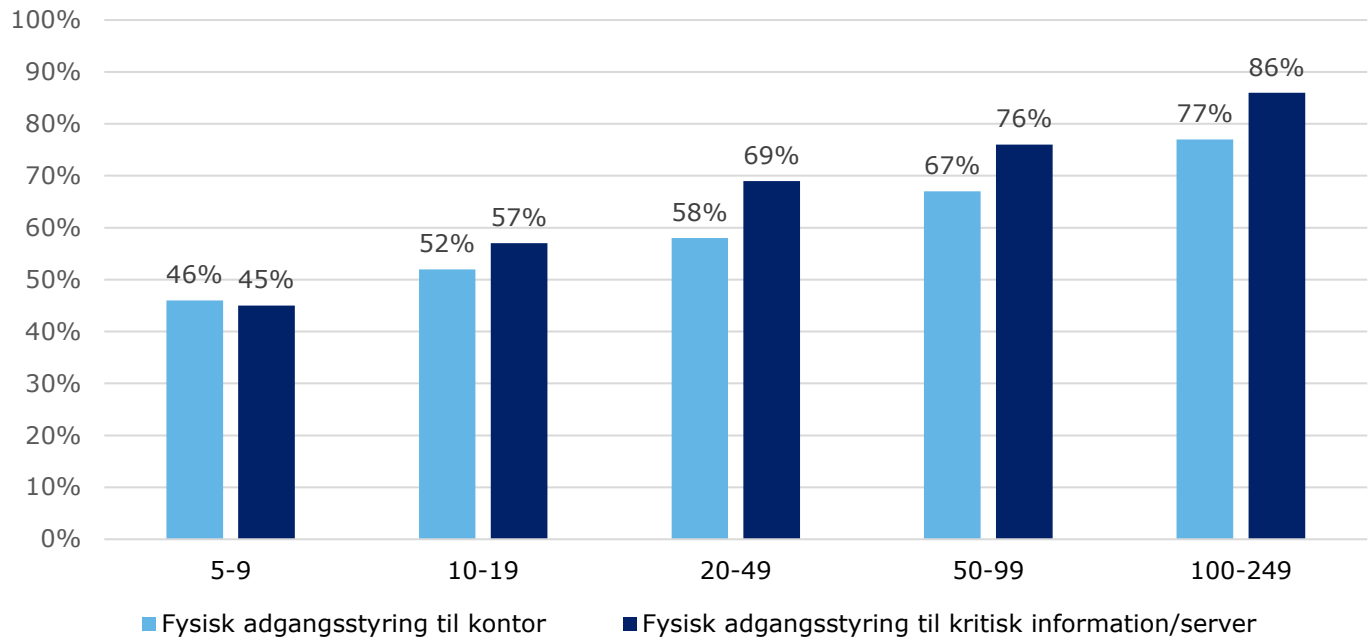


Kilde: Wilke for Monitor Deloitte

Som det fremgår af Figur 25, har kun 60 procent af virksomhederne sikret adgang til deres kritiske information, og 54 procent har sikret adgang til kontoret med personlig adgangsnøgle/-kort/-chip. Kobler man adgangskontrollen med, om virksomheden har outsourcet sin IT, fremgår det, at flere har adgangsstyring til servere og kritisk information, hvis de har outsourcet hele eller dele af deres IT.

4.8 Styring af fysisk adgang er i høj grad relateret til virksomhedens størrelse

Figur 26. Andel SMV'er, der har implementeret fysisk adgangsstyring på tværs af virksomhedsstørrelse



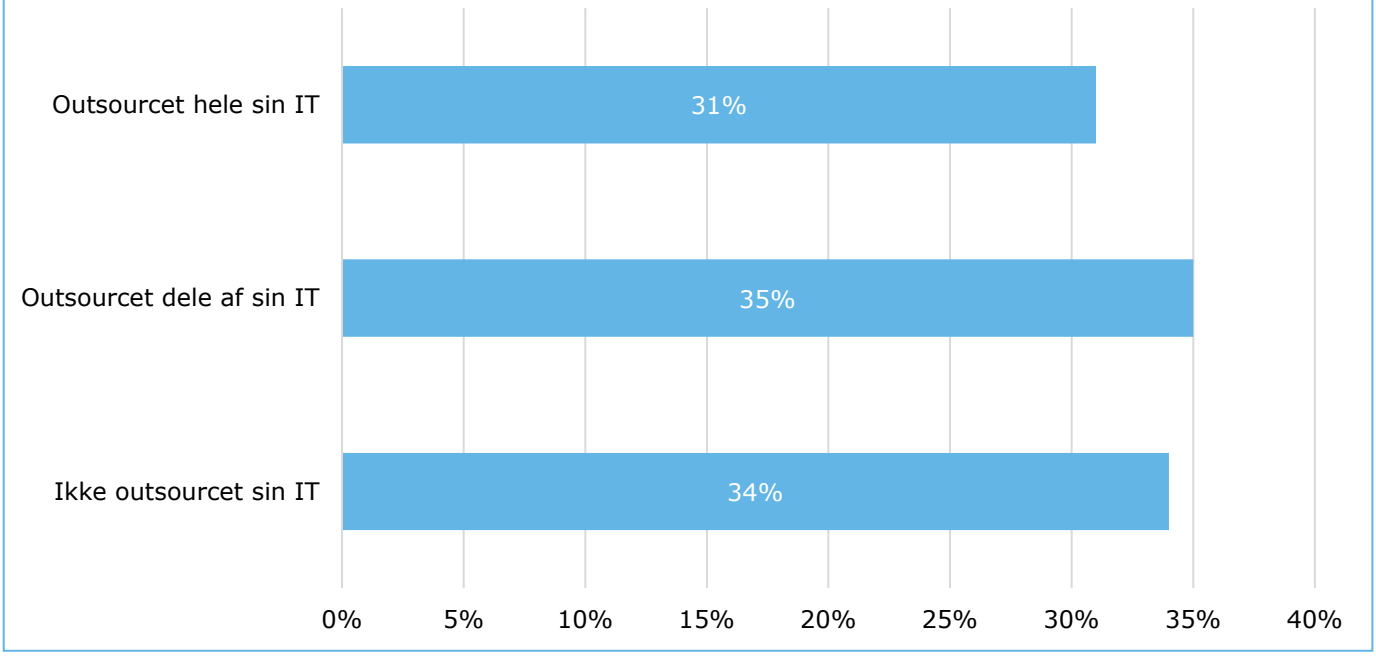
Kilde: Wilke for Monitor Deloitte

I Figur 26 er det vist, hvor stor en andel af virksomhederne der har fysisk adgangskontrol på tværs af virksomhedsstørrelse. Her ses det, at flere mindre virksomheder ikke har fysisk adgangskontrol. I caseinterviewene fremgår det, at mindre virksomheder i lavere grad har fysisk adgangskontrol, fordi de har færre medarbejdere, og det vil derfor være klart for medarbejderne, hvis der skulle komme nogen udefra ind på kontoret.

Outsourcing

Som SMV kan det være fordelagtigt at outsource sin IT-infrastruktur og IT-systemer. Virksomheder kan benytte outsourcing i varierende grad fra outsourcing af enkelte dele af virksomhedens infrastruktur til fuld outsourcing af alle IT-relaterede opgaver. Årsager til, at virksomhederne benytter sig af outsourcing af IT, kan blandt andet være, at virksomheden ikke har de fornødne kompetencer på området til selv at kunne etablere og drive den nødvendige infrastruktur. Det kan også være et ressourcespørgsmål, hvor de høje etableringsomkostninger erstattes af en månedlig ydelse til outsourcingpartneren. Ofte har SMV'er ikke en IT-afdeling eller en IT-ansvarlig, og det giver dermed god mening at placere disse kompetencer hos en ekstern samarbejdspartner. Flere af virksomhederne i caseinterviewene har outsourcet hele eller dele af deres IT, og flere af dem begrunder dette valg med, at de ikke mener, de internt har de nødvendige kompetencer, og at de derfor får adgang til flere IT-kompetencer såvel som flere IT-sikkerhedskompetencer ved at anvende en ekstern leverandør.

Figur 27. Andel SMV'er, der har outsourcet deres IT



Kilde: Wilke for Monitor Deloitte

Som det fremgår af Figur 27, har 31 procent af de danske SMV'er outsourcet hele deres IT, mens 35 procent har outsourcet dele af deres IT. Når man som virksomhed outsourcer hele eller dele af sin IT, lægger man også meget af sin IT-sikkerhed ud til sin outsourcingpartner.

Når man vælger at outsource hele eller dele af sin IT, er det vigtigt, at man stadig forholder sig til IT-sikkerhed, men til trods for dette er det kun 53 procent af de virksomheder, der har outsourcet hele deres IT, der har en databehandleraftale, mens tallet er 39 procent for de virksomheder, der har outsourcet dele af deres IT. Der findes flere vigtige tiltag i forhold til leverandørstyring på IT-sikkerhedsområdet. Andelen af SMV'er, der har en databehandleraftale, giver en indikation af, at mange SMV'er ikke er opmærksomme på dette.

4.9 Der er en sammenhæng mellem graden af outsourcing og ledelsens involvering

Det er tidligere blevet fremhævet, at ledelsens stillingtagen har stor betydning for virksomhedens IT-sikkerhed. Det viser sig også at have en relation til, om virksomheden har valgt at outsource sin IT. Af de 31 procent, der har outsourcet hele deres IT, har ledelsen i 48 procent af tilfældene i høj grad taget stilling til IT-sikkerhed, mens ledelsen i kun 2 procent af virksomhederne slet ikke har taget stilling til IT-sikkerhed. Af de 35 procent, der ikke har outsourcet deres IT, har ledelsen i 31 procent af tilfældene i høj grad taget stilling til IT-sikkerhed, mens ledelsen i hele 20 procent af tilfældene slet ikke har taget stilling til IT-sikkerhed. Denne sammenhæng indikerer, at når man vælger at outsource sin IT, har man ofte også forholdt sig til IT-sikkerhed, mens man i lavere grad har forholdt sig til IT-sikkerhed, når man ikke har outsourcet sin IT. Dette kan indikere, at hvis man som SMV har taget stilling til IT-sikkerhed, har man vurderet, at man ikke har de nødvendige kompetencer internt, og outsourcing ses derfor som et værktøj til at øge IT-sikkerheden.

En anden sammenhæng mellem outsourcing og IT-sikkerhed er, at virksomheder, der ikke har outsourcet deres IT, i lavere grad har implementeret de essentielle og grundlæggende tiltag end de virksomheder, der har outsourcet deres IT. Som det også forklares med valget af outsourcing, kan dette skyldes, at virksomheder, der ikke har out-

sourcet deres IT, i lavere grad har forholdt sig til IT-sikkerhed og derfor også i lavere grad har implementeret IT-sikkerhedsforanstaltninger.

Man kunne antage, at når man har outsourcet sin IT, overlader man i højere grad IT-sikkerheden til sin leverandør og forholder sig derfor i lavere grad til IT-sikkerhed relateret til medarbejderne. Der er dog ingen umiddelbar sammenhæng mellem disse to parametre.

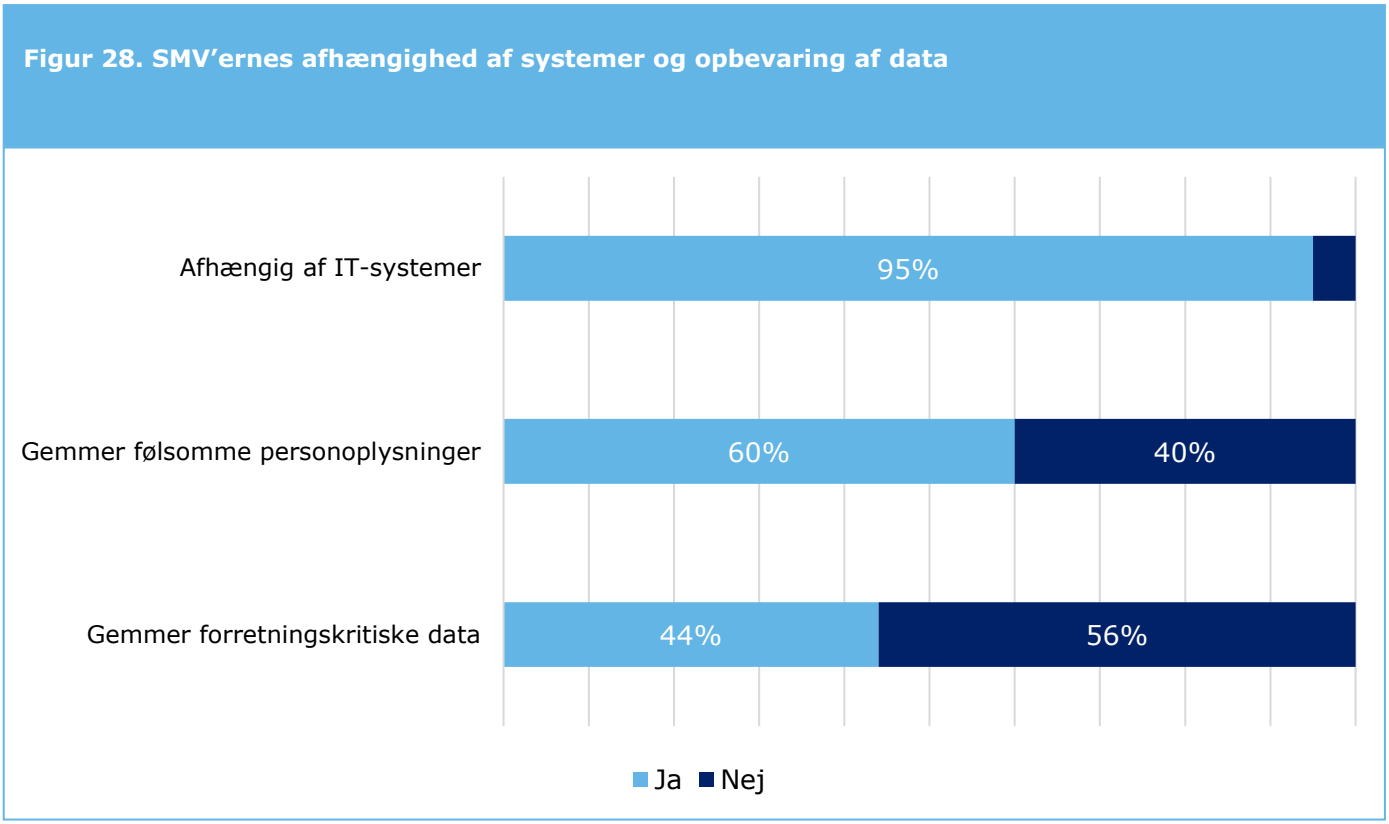
4.10 IT-sikkerhedsniveauet skal ses i relation til virksomhedens risikoprofil

For at kunne vurdere, om en virksomheds IT-sikkerhedsniveau er tilstrækkeligt, bør vurderingen tage virksomhedens risikoprofil i betragtning. Det vil sige, at vurderingen skal være en kombination af, hvor alvorligt et IT-sikkerhedsbrud vil være for virksomheden, og hvor stor sandsynligheden er for, at virksomheden bliver ramt.

Virksomhedens risikoprofil er grundlæggende afhængig af tre parametre:
1. I hvilken grad virksomheden er afhængighed af IT-systemer i forhold til virksomhedens daglige drift.
2. I hvilken grad virksomheden gemmer følsomme personoplysninger.
3. I hvilken grad virksomheden er afhængig af forretningskritiske data (fx patenter og intellektuelle rettigheder).

Derudover inddrages branchen også til at vurdere virksomhedernes risikoprofil, da nogle brancher er mere yndede mål for IT-kriminelle end andre, for eksempel den finansielle sektor. Yderligere beskrivelse fremgår af appendiks 7.1.7.

Figur 28. SMV'ernes afhængighed af systemer og opbevaring af data



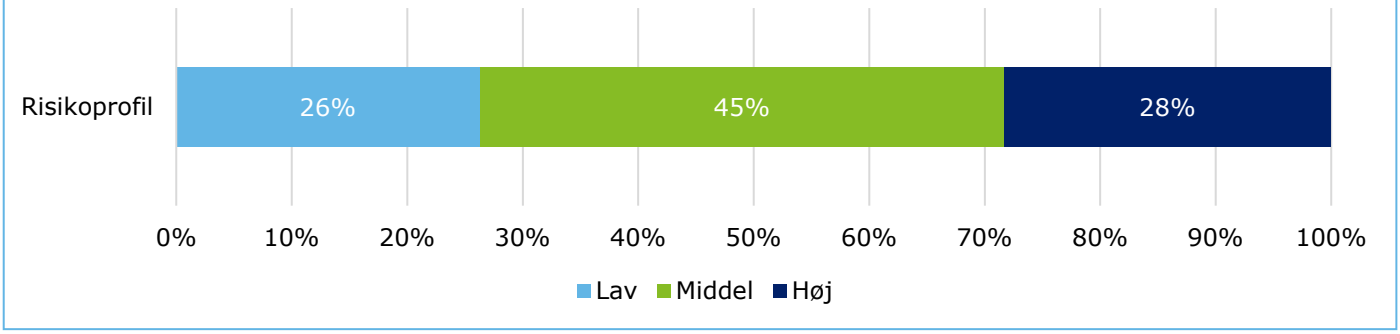
Kilde: Wilke for Monitor Deloitte

På tværs af det danske SMV-segment er der stor afhængighed af IT-systemer, jf. Figur 28. 95 procent af de danske SMV'er er afhængige af IT-systemer i forhold til deres drift. Heraf svarer 70 procent, at de har stor afhængighed af deres IT-systemer. Dermed må det siges, at danske SMV'er generelt anser deres systemer for at være kritiske, fordi de vil blive påvirket i tilfælde af et IT-sikkerhedsbrud, der påvirker driften. Figur 28 viser ligeledes, at 60 procent og 44 procent gemmer henholdsvis følsomme personoplysninger og forretningskritiske data. For de virksomheder, der gemmer disse typer data, kan et sikkerhedsbrud være meget kritisk, fordi det kan betyde læk af fortrolige data, eller at man mister adgang til information, der er central for virksomhedens drift. Af de 44 procent af

virksomhederne, der svarer, at de gemmer forretningskritiske data, svarer 36 procent, at læk af forretningskritiske data vil betyde, at de mister deres forretningsgrundlag. Dette svarer til 16 procent af den samlede population, der dermed ville miste deres forretningsgrundlag og potentielt gå konkurs, hvis de fik stjålet eller kompromitteret deres forretningskritiske data.

Blandt de danske SMV'er er der derfor stor forskel på, hvor kritisk et sikkerhedsbrud vil være. For nogle virksomheder vil datalæk eller systemnedbrud være særlig kritisk for deres forretning, mens andre virksomheder ikke vil blive påvirket i lige så høj grad. For at gøre det muligt at vurdere, hvor udsat en virksomhed er i forbindelse med et IT-sikkerhedsangreb, anvendes der i denne rapport en model, hvormed virksomhederne inddeles i tre risikoprofiler: lav, middel og høj risikoprofil.

Figur 29. SMV'ernes fordeling indenfor risikoprofil

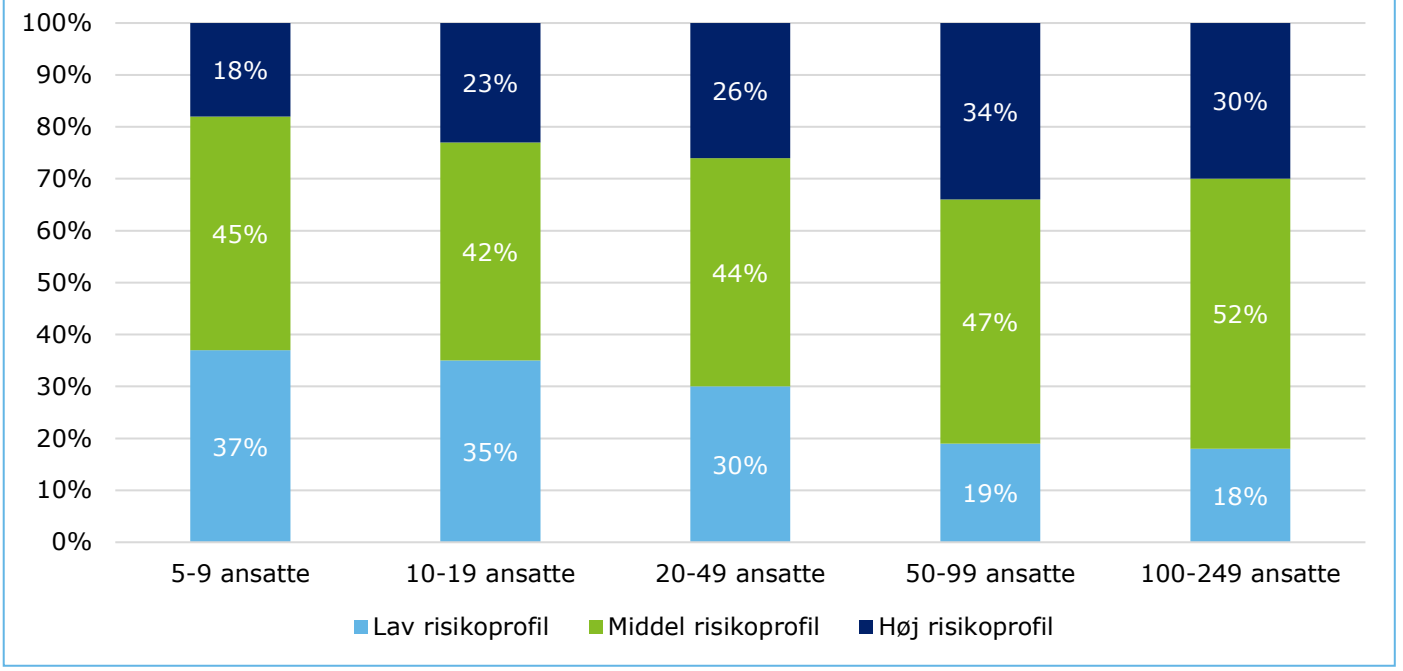


Kilde: Wilke for Monitor Deloitte og Monitor Deloitte-analyse

Når man ser på SMV'ernes risikoprofil, har størstedelen af virksomhederne en middel risikoprofil, som det fremgår af Figur 29. Virksomheder med lav og høj risikoprofil udgør nogenlunde to lige store grupper.

Man kan også se på risikoprofilen på tværs af virksomhedernes størrelse. Der ses en sammenhæng mellem virksomhedsstørrelsen og virksomhedens risikoprofil.

Figur 30. Sammenhængen mellem SMV'ernes størrelse og risikoprofil



Kilde: Wilke for Monitor Deloitte og Monitor Deloitte-analyse

Af Figur 30 ser der en tendens til, at jo større virksomheden er, jo højere risikoprofil har den, hvilket indikerer, at større virksomheder er mere afhængige af IT-systemer og mere følsomme data.

Hvis man holder virksomhedens iværksatte IT-sikkerhedstiltag op imod virksomhedens risikoprofil, er det muligt at vurdere, om virksomheden har et passende IT-sikkerhedsniveau. Dette skyldes, at virksomhederne kan have forskellige behov for IT-sikkerhed afhængigt af risikoprofil. IT-sikkerhedsniveauet afspejler således, hvor robust virksomhedens informationssikkerhed er, og hvor godt virksomheden er beskyttet mod et eventuelt IT-sikkerhedsangreb.

Baseret på risikoprofilen og virksomhedens IT-sikkerhedsniveau er det muligt at definere tre arketyper for virksomhederne, der vil blive anvendt videre i denne rapport. Kategorierne er:

1. **De påpasselige SMV'er:** Virksomheder med et IT-sikkerhedsniveau, der er *mere end tilstrækkeligt* i forhold til deres risikoprofil.
2. **De tilpas sikrede SMV'er:** Virksomheder med et IT-sikkerhedsniveau, der er *tilstrækkeligt* i forhold til deres risikoprofil.
3. **De sårbare SMV'er:** Virksomheder med et IT-sikkerhedsniveau, der *ikke er tilstrækkeligt* i forhold til deres risikoprofil.

4.11 39 procent af danske SMV'er kan kategoriseres som sårbare overfor IT-sikkerhedshændelser

På baggrund af ovenstående er det muligt at vurdere, om danske SMV'er har et tilstrækkeligt IT-sikkerhedsniveau. Det vil sige en passende mængde foranstaltninger, processer, viden m.m., der gør virksomheden i stand til at imødegå et IT-sikkerhedsangreb og således være bedre i stand til at forebygge IT-sikkerhedsbrud. Sammenhængen mellem virksomhedernes IT-sikkerhedsniveau og deres risikoprofil fremgår af Tabel 3.

Tabel 3. SMV'ers vægtede fordeling indenfor arketyperne

		IT-sikkerhedsniveau		
		Lavt	Middel	Højt
Risikoprofil	Høj	**De sårbare SMV'er:** 7 procent	**De sårbare SMV'er:** 9 procent	**De tilpas sikrede SMV'er:** 6 procent
	Middel	**De sårbare SMV'er:** 23 procent	**De tilpas sikrede SMV'er:** 15 procent	**De påpasselige SMV'er:** 6 procent
	Lav	**De tilpas sikrede SMV'er:** 25 procent	**De påpasselige SMV'er:** 8 procent	**De påpasselige SMV'er:** 1 procent

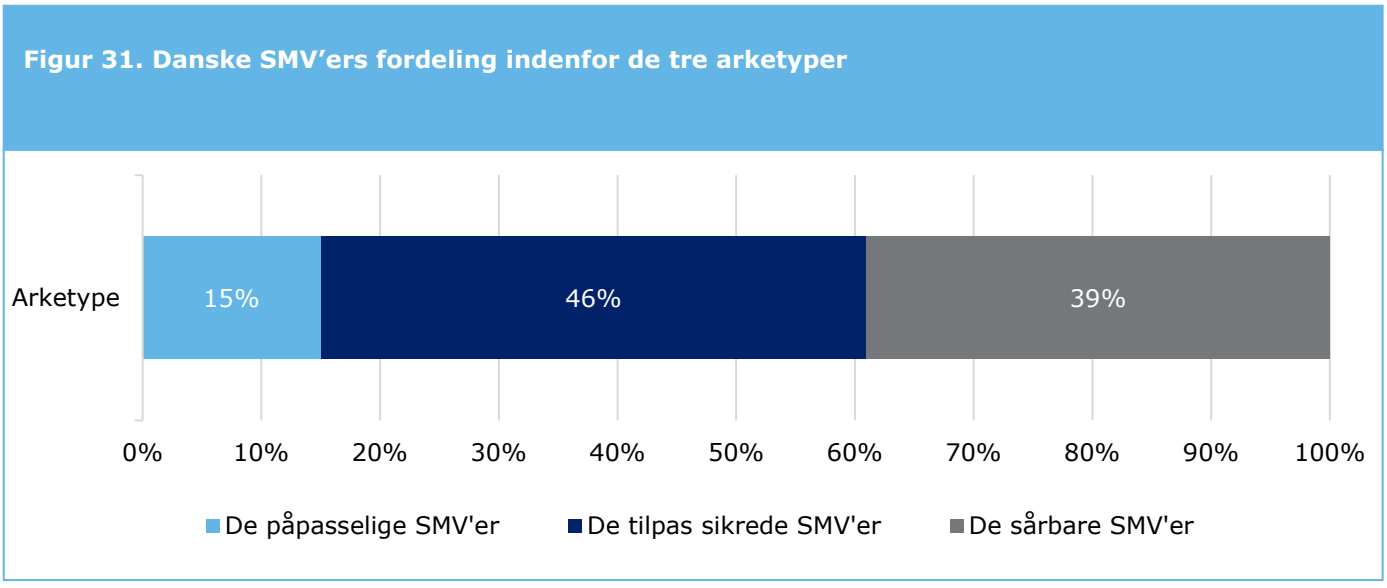
Kilde: Wilke for Monitor Deloitte og Monitor Deloitte-analyse

Denne vurdering viser følgende fordeling:

- **De påpasselige SMV'er:** 15 procent af de danske SMV'er har et IT-sikkerhedsniveau, der er mere end tilstrækkeligt i forhold til deres risikoprofil (fremgår af de lyseblå bokse).
- **De tilpas sikrede SMV'er:** 46 procent af de danske SMV'er har et IT-sikkerhedsniveau, der er tilstrækkeligt i forhold til deres risikoprofil (fremgår af de mørkeblå bokse).
- **De sårbare SMV'er:** 39 procent af de danske SMV'er har et IT-sikkerhedsniveau, der ikke er tilstrækkeligt i forhold til deres risikoprofil (fremgår af de grå bokse).

Dette fremgår ligeledes af Figur 31 herunder, der er en aggregering af data fra Tabel 3.

Figur 31. Danske SMV'ers fordeling indenfor de tre arketyper



Kilde: Wilke for Monitor Deloitte og Monitor Deloitte-analyse

Det, der kendetegner de forskellige arketyper, er:

- **De påpasselige SMV'er – virksomheder, hvor IT-sikkerhedsniveauet er mere end tilstrækkeligt:** Denne arketype har den laveste grad af afhængighed af følsomme data. Blot 28 procent svarer, at deres systemer behandler forretningskritiske data. Omvendt har alle virksomhederne sikret grundlæggende foranstaltninger og flere avancerede tiltag. For eksempel gennemfører 35 procent af disse virksomheder kontinuerligt måling af medarbejdernes bevidsthed om IT-sikkerhedstrusler (dette er henholdsvis 16 procent og 13 procent for de an-

dre arketyper). Ledelsen har i højere grad taget stilling til IT-sikkerhed end ledelsen i de andre arketyper, mens medarbejderne også inddrages mere, idet 72 procent kommunikerer deres IT-sikkerhedspolitik (mod 37 procent for arketype 3), og 33 procent måler på medarbejdernes bevidsthed om sikkerhedstrusler. De påpasselige SMV'er er godt rustede mod IT-sikkerhedsangreb og vil typisk også være på forkant med potentielle IT-sikkerhedstrusler, men der er også en risiko for, at virksomhederne har overimplementeret og derfor har brugt for mange ressourcer på IT-sikkerhed.

- **De tilpas sikrede SMV'er – virksomheder, hvor IT-sikkerhedsniveauet er tilstrækkeligt:** Denne arketype har en meget varierende anvendelse af data og systemer og ligger i mellemkategorien i forhold til de to andre arketyper. I 40 procent af disse virksomheder har man forretningskritiske data. Hvad angår foranstaltninger og involvering af medarbejdere og ledelse, er denne kategori ligeledes varierende på tværs af de tre parametre. Et kendetegn ved virksomhederne i denne kategori er, at de har et IT-sikkerhedsniveau på niveau med eller en anelse højere end virksomhederne i arketype 3, men de har en lavere risikoprofil. De tilpas sikrede SMV'er har et IT-sikkerhedsniveau, der matcher deres risikoprofil, og de har derfor implementeret det rette niveau af IT-sikkerhed.
- **De sårbare SMV'er – virksomheder, hvor IT-sikkerhedsniveauet ikke er tilstrækkeligt:** Alle virksomhederne har en stor afhængighed af deres systemer i deres daglige drift og er samtidig afhængige af en eller flere typer følsomme data. For eksempel svarer 72 procent af respondenterne i denne gruppe, at de behandler forretningskritiske data, hvilket er det højeste niveau for de tre arketyper. På trods af den store afhængighed af systemer og data har mange af virksomhederne ikke styr på grundlæggende IT-foranstaltninger, for eksempel backupprocedurer og løbende opdatering af systemer. Blot 57 procent af virksomhederne i denne arketype svarer ja til, at de gennemfører systematisk og løbende opdatering af systemer og programmer. Medarbejdere og ledelse er i lavere grad tænkt ind i IT-sikkerheden i denne type virksomheder. De sårbare SMV'er har et for lavt IT-sikkerhedsniveau i forhold til deres risikoprofil og er derfor særlig udsatte i tilfælde af et IT-sikkerhedsangreb og er i risiko for, at et IT-sikkerhedsangreb kan blive til et IT-sikkerhedsbrud, der kan få store konsekvenser. Det er værd at bemærke, at 7 procent af de sårbare SMV'er har et lavt IT-sikkerhedsniveau og en høj risikoprofil, hvilket gør dem meget udsatte for IT-sikkerhedsangreb.

4.12 Opsummering

Kapitel 4 viser, at 39 procent af danske SMV'er ikke har et IT-sikkerhedsniveau, der i tilstrækkelig grad matcher deres risikoprofil. IT-sikkerhedsniveauet udgøres af tre elementer: IT-sikkerhed relateret til medarbejdere og ledelse, IT-sikkerhedsforanstaltninger og fysisk adgangskontrol.

Når man ser på IT-sikkerhed relateret til medarbejdere, bruger virksomhederne ikke formaliserede tiltag, men fokuserer mest på den mundtlige kommunikation til medarbejderne. Formaliserede tiltag, for eksempel en dokumenteret IT-sikkerhedspolitik, anvendes generelt af en mindre del, men der ses dog en tendens til, at større virksomheder arbejder mere formaliseret med IT-sikkerhed, idet en større del træner deres medarbejdere og også har en dokumenteret IT-sikkerhedspolitik. Overordnet set har ledelsen i en stor andel af virksomhederne til en vis grad, i nogen grad eller i høj grad taget stilling til IT-sikkerhed, og når man ser dette i relation til virksomhedernes IT-sikkerhedsniveau, er der en indikation af, at i jo højere grad ledelsen har taget stilling til IT-sikkerhed, jo højere er virksomhedens IT-sikkerhedsniveau.

IT-sikkerhedsforanstaltninger dækker grundlæggende og avancerede IT-sikkerhedsforanstaltninger, hvor der under de grundlæggende er nogle helt essentielle IT-sikkerhedsforanstaltninger. Ser man på tværs af de to essentielle IT-sikkerhedsforanstaltninger, har knap en fjerdedel af virksomhederne ikke implementeret begge disse. Ser man på de resterende grundlæggende tiltag, har 49 procent af virksomhederne ikke implementeret dem, mens der til gengæld er en relativt stor andel, der har implementeret de avancerede tiltag.

Det sidste element af en virksomheds IT-sikkerhedsniveau er den fysiske adgangskontrol, og her viser det sig, at kun 60 procent af virksomhederne har fysisk adgangskontrol i forhold til deres kritiske information og/eller servere. Det er særligt virksomheder, der har outsourcet deres IT, der har adgangskontrol, hvilket kan hænge sammen med, at virksomhedernes outsourcingpartnere har implementeret dette. Derudover er fysisk adgangskontrol relateret til virksomhedens størrelse, da flere af de større virksomheder har fysisk adgangskontrol end de mindre virksomheder.

5 Barrierer og drivkræfter for at øge IT-sikkerhedsniveauet i danske SMV'er

Danske SMV'er oplever en lang række udfordringer i arbejdet med IT-sikkerhed, hvor særligt medarbejdere, ledelsen og viden om IT-sikkerhed spiller en rolle. Virksomhederne oplever, at virksomhedskulturen er et centralt element, når man arbejder med IT-sikkerhed, og at kommunikation er vigtig for at forankre IT-sikkerhed i virksomhedskulturen. Derudover er samarbejde med eksterne en måde at øge bevidstheden omkring IT-sikkerhed og kan være en kilde til øget IT-sikkerhed, hvis virksomheden ikke selv har de nødvendige kompetencer. Virksomhederne oplever dog også for eksempel lovgivning som en drivkraft for arbejdet med at styrke IT-sikkerhed.

Spørgeskemaundersøgelsen afdækkede IT-sikkerhedsniveauet for danske SMV'er, som viste, at næsten 40 procent af virksomhederne falder i kategorien *sårbare*. Der blev også gennemført 14 kvalitative interview for at identificere barrierer og drivkræfter for virksomhedernes arbejde med IT-sikkerhed. Interviewene var med SMV'er i forskellige brancher med enten middel eller højt IT-sikkerhedsniveau. Casevirksomhederne er beskrevet i afsnit 7.4.

Barrierer skal ses som de udfordringer, virksomhederne møder i deres arbejde med at øge IT-sikkerheden, og som virksomhederne er nødt til at adressere for at kunne øge virksomhedens IT-sikkerhed. Manglende økonomi kan eksempelvis være en barriere for at kunne investere i IT-sikkerhed. I visse tilfælde kan en barriere vendes til en drivkraft, mens det i andre tilfælde blot handler om at nedbryde barrieren for arbejdet. Manglende engagement fra ledelsens side i forhold til IT-sikkerhed kan for eksempel være en barriere, men hvis ledelsen engagerer sig i IT-sikkerhed, kan det fungere som en drivkraft.

Når man taler med danske SMV'er, står særligt tre barrierer frem: medarbejderne, ledelsen og prioriteringen af ressourcer. Medarbejderne og ledelsen opfattes i særlig grad som barrierer for IT-sikkerhed, når de mangler viden og information om området, og her bliver uformel kommunikation et centralt middel til at nedbryde disse barrierer. Når medarbejderne og ledelsen besidder viden om IT-sikkerhed, bliver det i højere grad til en drivkraft, hvilket også gælder for de IT-ansvarlige i SMV'erne. De IT-ansvarlige oplever dog også, at det til tider kan være svært at navigere i informationen på området. Dette overkommes tit ved at lytte til og modtage råd fra eksterne samarbejdspartnere som eksempelvis en outsourcingpartner eller et IT-sikkerhedsrådgivningsfirma. Ligeledes oplever SMV'erne, at virksomhedens risikoprofil bliver en drivkraft for at arbejde med IT-sikkerheden, idet man har identificeret, at et sikkerhedsbrud kan få store konsekvenser for virksomheden. Hvis risikoprofilen skal blive en drivkraft kræver det dog, at virksomheden foretager en konkret risikovurdering. Enkelte af de interviewede virksomheder har også haft et IT-sikkerhedsbrud, hvor de oplevede konsekvenserne ved dette og derfor øgede deres indsats indenfor IT-sikkerhed. Slutteligt kunne man forvente, at kundernes krav til IT-sikkerhed ville blive en drivkraft for IT-sikkerhed, men kun få virksomheder vurderer, at det er tilfældet. Alle virksomheder vil i udgangspunktet blive påvirket af persondataforordningen, men der er også enkelte SMV'er, der er underlagt særlige regler på området, og lovgivningen bliver således også en drivkraft for virksomhedens fokus på området.

De efterfølgende afsnit går i dybden med de enkelte elementer, virksomhederne peger på.

5.1 Medarbejdernes handlinger skaber udfordringer for arbejdet med IT-sikkerhed

Som beskrevet i kapitel 4 er medarbejderne et vigtigt element i en virksomheds IT-sikkerhed. Hovedparten af de adspurgte casevirksomheder oplever imidlertid også, at medarbejdernes handlinger og manglende viden om IT-sikkerhed kan være en barriere i deres arbejde med IT-sikkerhed. Medarbejderne ses i visse virksomheder som det svageste led i forhold til IT-sikkerheden, idet der kan slippe trusler forbi de tekniske foranstaltninger, og således er det kun medarbejderne, der i sidste ende kan agere værn mod IT-sikkerhedsangreb.

Medarbejdernes manglende omstillingsparathed er en af de barrierer, virksomhederne oplever i arbejdet med IT-sikkerhed. I forbindelse med implementeringen af visse IT-sikkerhedsrelaterede tiltag er det nødvendigt at ændre på processer og arbejdsgange og således implementere forandringer for medarbejderne. Disse forandringer kan for eksempel være, hvis der indføres kvartalsvise fornyelser af medarbejdernes adgangskoder til deres computere, eller at medarbejderne ikke længere må anvende USB-nøgler til at dele filer med eksterne parter. I Maskinhandler Indkøbsringen oplever man, at medarbejderne kan være en udfordring, fordi de ikke altid er åbne for de forandringer, det kræver at implementere nye IT-sikkerhedstiltag. Her forsøger man derfor i størst mulig grad at undgå at forstyrre medarbejdernes arbejdsgange.

5.1.1 IT-sikkerhed skal forankres i virksomhedskulturen for at opnå tilstrækkelig fokus og opmærksomhed

Flere af casevirksomhederne påpeger, at medarbejdernes adfærd og videnniveau var en barriere for deres arbejde med IT-sikkerhed, og man kan se denne udfordring som værende kulturelt forankret, og flere af virksomhederne påpeger, at virksomhedskulturen er en barriere i arbejdet med IT-sikkerhed. Dette var også tilfældet i TP Aerospace, hvor virksomhedskulturen var en udfordring i arbejdet med at udbrede anvendelsen af IT-sikkerhedsforanstaltninger, som det præsenteres i Case 5. TP Aerospace kom fra et punkt, hvor man ingen IT-sikkerhed havde, og hvor processen mod at øge IT-sikkerheden krævede meget kommunikation til medarbejderne.

TP Aerospace om virksomhedskulturen som en barriere for IT-sikkerhed

Navn | TP Aerospace

Branche | Handel

Størrelse | 220 medarbejdere

IT-sikkerhedsniveau | Middel

Risikoprofil | Lav

TP Aerospace sælger flyhjul og -bremser til mindre fly- og fragtselskaber og henvender sig til internationale markeder.

Da man hos TP Aerospace for nylig oprettede en IT-afdeling, havde virksomheden et begrænset IT-sikkerhedsniveau. Da den nye IT-ansvarlige kom til virksomheden, påbegyndte han arbejdet med IT-sikkerhed. I processen med at øge niveauet har medarbejdernes handlinger og begrænsede viden om IT været en barriere for arbejdet med IT-sikkerhed, da medarbejderne ikke altid har været indstillet på de forandringer, det har krævet. For eksempel indførte den nye IT-ansvarlige password på alle medarbejderes computere, hvilket medarbejderne indledningsvis ikke brød sig om. Generelt var det forandringer, som ændrede i medarbejdernes arbejdsgange eller begrænsede dem, i forhold til hvad de tidligere havde kunnet. Derfor bruger man i virksomheden en del tid på at kommunikere forandringer, herunder informere medarbejderne, inden forandringerne implementeres, og om hvorfor forandringerne er nødvendige. Man har fra IT-afdelingens side for eksempel udarbejdet et nyhedsbrev og en blog, som man bruger til at kommunikere forandringerne.

Arbejdet med IT-sikkerhed krævede en kulturændring blandt medarbejderne i forhold til at skabe en større forståelse af IT og i forhold til at gøre IT-sikkerhed til en mere naturlig del af arbejdet. Den indledende tilgang til IT og IT-sikkerhed havde været en del af virksomheden fra begyndelsen, hvorfor det var så

Case 5. TP Aerospace

Arbejdet med virksomhedskulturen er centralt for at overkomme den barriere, som medarbejdernes handlinger og manglende viden kan udgøre. Dette var der også fokus på i Sund & Bælt, hvor man igennem uformel kommunikation forsøgte at skabe en kultur med større åbenhed, hvor det var i orden at stille spørgsmål om IT-sikkerhed og spørge om råd og vejledning, når man var i tvivl. Man forsøgte samtidig løbende at forklare, hvorfor man foretog ændringer og holdt fokus på de positive konsekvenser, som IT-sikkerhedsrelaterede tiltag ville medføre. Først da man nåede et vist viden- og forståelsesniveau blandt medarbejderne i Sund & Bælt, var man klar til at implementere formelle tiltag som uddannelses- og træningsprogrammer indenfor IT-sikkerhed. Havde Sund & Bælt i stedet indledt indsatsen i forhold til IT-sikkerhed med formel træning, er det ikke sikkert, det havde haft samme effekt, fordi man ikke først havde forankret IT-sikkerhed i virksomhedskulturen. Derudover skaber kommunikationen en grundlæggende forståelse for IT-sikkerhed. Ud fra caseinterviewene blev det klart, at rækkefølgen af en virksomheds IT-sikkerhedsrelaterede tiltag er afgørende for at lykkes med indsatsen. For at sikre, at der er et fundament for forståelsen af IT-sikkerhed, kan det være hensigtsmæssigt at starte med tiltag, der ikke er formaliserede, inden man arbejder videre med de formaliserede tiltag.

Den uformelle kommunikation er et middel til at ændre virksomhedskulturen, men for at opnå denne ændring til fulde, er det vigtigt, at kommunikationen tilpasses medarbejdere og forskellige medarbejdergrupper. For at gøre IT-sikkerhed mere håndgribelig er der derfor flere af virksomhederne, der bruger eksempler på IT-sikkerhedsbrud fra andre virksomheder. Det er for eksempel tilfældet i casevirksomheden Fremtidens Læring, hvor man inddrager eksempler fra medierne i den interne kommunikation og på den måde gør IT-sikkerhed mere håndgribelig og kontekstuel for medarbejderne. Udover at anvende eksempler fra andre virksomheder er det også vigtigt, at kommunikationen tilpasses medarbejderne, og det er afgørende, at kommunikationen tilpasses det faglige område, medarbejderne arbejder indenfor. I casevirksomheden Blå Maritim har medarbejderne meget forskellige baggrunde og for at imødekomme dette, har virksomheden en generel kommunikation om IT-sikkerhed. Derudover inddrager man afdelingslederne i de enkelte afdelinger, så de bliver bindeleddet mellem den generelle IT-sikkerhed og afdelingen.

Medarbejdernes brugeradfærd i deres privatsfære er ofte dybt forankret i dem og flyder derfor over i virksomhedens kultur. Det er således nødvendigt, at virksomhederne i deres kommunikation lægger vægt på, hvorfor det er nødvendigt at agere anderledes på sit arbejde end privat. I Fremtidens Læring så man, at medarbejdernes adfærd i deres privatliv havde en stor effekt på IT-kulturen i virksomheden. Derfor lagde man i kommunikationen til medarbejderne meget vægt på, hvordan man bruger IT og internettet i en professionel sammenhæng, da det kan få store konsekvenser for virksomheden, hvis man ikke er betænksom og agerer forsvarligt.

Det kan umiddelbart være svært at vurdere, om man har formået at skabe den nødvendige opmærksomhed om IT-sikkerhed og har opnået den ønskede kulturændring. To af de adspurgte virksomheder forsøger derfor at måle udviklingen i medarbejdernes bevidsthed om IT-sikkerhed over tid, for eksempel ved at gennemføre phishingtest, som man har gjort i Danmarks Naturfredningsforening. Man simulerede et phishingangreb for at teste niveauet for medarbejdernes IT-sikkerhedskendskab i forhold til phishingmails. Testen blev brugt til at vurdere niveauet og til at vurdere, om indsatsen havde den ønskede effekt. Derudover blev testen også anvendt i den videre kommunikation af IT-sikkerhed, hvilket var med til at øge fokus blandt medarbejderne og skabe en større forståelse af, hvad IT-sikkerhedstruslen bestod i.

At uformel kommunikation er et centralt redskab til at sikre en kulturændring i forhold til IT-sikkerhed underbygges af, at 74 procent af SMV'erne kommunikerer informationssikkerhed mundtligt, mens man i mindre grad bruger formaliserede tiltag. Deloitte Cyber Risk anbefaler, at man kontinuerligt gør medarbejderne opmærksomme på IT-sikkerhed; det er ikke nødvendigvis metoden, der er den vigtigste, men derimod frekvensen. Deloitte Cyber Risk oplever dog, at formaliseret træning og måling af medarbejdernes bevidsthed kan være gode værktøjer til at nå ud til medarbejderne. Af indeværende undersøgelser fremgår det, at kun 14 procent af de danske SMV'er kontinuerligt måler deres medarbejderes bevidsthed om IT-sikkerhedstrusler.

5.2 Ledelsens manglende involvering er en barriere for virksomhedens IT-sikkerhedsniveau og er ofte et resultat af manglende viden på området

Ledelsen anses for at være en afgørende faktor i relation til IT-sikkerhed, da den udover at allokere de nødvendige ressourcer også har en stor rolle i at drive agendaen internt i virksomheden. I kapitel 4 blev det vist, hvordan ledelsens stillingtagen til IT-sikkerhed var essentiel for, at man som virksomhed havde implementeret diverse IT-sikkerhedsforanstaltninger og andre IT-sikkerhedsrelaterede tiltag, herunder træning af medarbejdere. Ledelsens videnniveau kan således både fungere som en barriere og drivkraft i arbejdet med IT-sikkerhed, idet et tilstrække-

ligt videnniveau vil betyde, at de ser behovet for IT-sikkerhed. Hvis ledelsen ikke i tilstrækkelig grad prioriterer IT-sikkerhed, bliver de en barriere, da de nødvendige ressourcer ikke allokeres til at implementere tiltag på området. Flere virksomheder peger på, at når ledelsen ikke engagerer sig i IT-sikkerhed, skyldes det, at de i højere grad fokuserer på det kommercielle og derudover ikke har tilstrækkelig viden om IT-sikkerhed til at engagere sig.

Hvis ledelsen engagerer sig i IT-sikkerhed, kan de blive en vigtig drivkraft for øget IT-sikkerhed. I denne sammenhæng ses ledelsens videnniveau indenfor IT-sikkerhed som værende central i at sikre ledelsens engagement. Fire af de adspurgte virksomheder ser ledelsens manglende engagement som en barriere for deres arbejde med IT-sikkerhed, når de ikke i tilstrækkelig grad ved, hvad IT-sikkerhed indebærer. De oplever dog også, at når ledelsen er tilstrækkelig informeret om IT-sikkerhed, vil de være villige til at investere i området og implementere de nødvendige foranstaltninger. Dette var blandt andet tilfældet i Juhls Fabrik, hvor man så ledelsens forståelse af IT-sikkerhed som central for at kunne drive arbejdet med IT-sikkerhed, og man havde derfor stort fokus på at kommunikere til ledelsen, som det fremgår af Case 6.

Juhls Fabrik om ledelsen som en barriere for IT-sikkerhed

Navn | Juhls Fabrik

Branche | Industri

Størrelse | 250 medarbejdere

IT-sikkerhedsniveau | Høj

Risikoprofil | Høj

Juhls Fabrik er en dansk produktionsvirksomhed, der sælger til andre virksomheder.

I Juhls Fabrik oplevede man, at der var for lidt fokus på IT-sikkerhed fra ledelsens side, og at en barriere for IT-sikkerhed var ledelsens manglende viden om IT-sikkerhed. Da ledelsen ikke havde en tilstrækkelig viden om IT-sikkerhed, så den ikke et behov for viden om IT-sikkerhed, og den var derfor ikke villig til at investere heri. I takt med at Juhls Fabrik voksede, kom der flere ledere i virksomheden, heriblandt nogle, der generelt havde mere fokus på IT-sikkerhed. Derudover havde de IT-ansvarlige fokus på at forklare de konsekvenser, det kunne have, hvis man oplevede et IT-sikkerhedsangreb. Som et led i denne kommunikation fik man en ekstern aktør til at udarbejde en IT-sikkerhedsanalyse, som kunne bruges i kommunikationen. Man oplevede, at det gav stor værdi at få et eksternt perspektiv på IT-sikkerheden. Det gjorde det nemmere at kommunikere IT-sikkerhed, da det gjorde hullerne mere håndgribelige, og det øgede ledelsens forståelse for IT-sikkerhed og dermed villighed til at investere i området.

Case 6. Juhls Fabrik

For at øge ledelsens engagement i IT-sikkerhed er det vigtigt at informere ledelsen om IT-sikkerhed og eventuelle konsekvenser ved manglende IT-sikkerhed. Som det er tilfældet i forbindelse med kommunikation til medarbejderne, kan dette ske gennem mundtlig kommunikation, hvor man kontinuerligt skubber information til ledelsen. Derudover kan en ekstern IT-sikkerhedsanalyse være et værktøj i kommunikationen om IT-sikkerhed, som det blev for Juhls Fabrik. Fem af de andre adspurgte virksomheder brugte også denne tilgang og fik foretaget en IT-revision eller IT-sikkerhedsanalyse. Dette var blandt andet tilfældet for Maskinhandler Indkøbsringen, hvor man havde succes med en ekstern IT-sikkerhedsanalyse, der havde en god virkning på ledelsen, fordi IT-sikkerhedsanalysen gjorde det mere håndgribeligt og dermed lettere at kommunikere til ledelsen. En ekstern analyse gør den kommunikative opgave lettere, og det styrker også budskabet, at det kommer fra en ekstern aktør. Secure Service anvendte ligesom Juhls Fabrik og Maskinhandler Indkøbsringen en ekstern sikkerhedsanalyse og oplevede, at ledelsen på baggrund af IT-revisionen blev mere opmærksom på IT-sikkerheden. IT-afdelingen oplevede faktisk, at ledelsen henvendte sig til IT-afdelingen for at finde ud af, hvad der skulle gøres, i stedet for at IT-afdelingen skulle skubbe IT-sikkerhedsagendaen selv.

Udover den interne kommunikation kan den øgede information også komme fra andre kilder, og flere af virksomhederne nævner, at den øgede fokus på IT-sikkerhed i medierne har øget ledelsens forståelse for IT-sikkerhed, som det for eksempel var tilfældet for AB Hjem. Her var der tidligere en lav grad af fokus på IT-sikkerheden hos ledelsen, men den øgede opmærksomhed om IT-sikkerhed i medierne ændrede også fokus hos ledelsen. Det har betydet, at ledelsen har været mere villig til at afsætte flere ressourcer til IT-sikkerhed, og at den generelt er mere

opmærksom på IT-sikkerhed i virksomheden. Andre eksterne kilder kan også være ledelsens eget netværk, hvor ledelsen taler med andre ledere, der har erfaringer med IT-sikkerhed eller har oplevet et IT-sikkerhedsbrud.

5.3 Viden om IT-sikkerhed er definerende for virksomhedens IT-sikkerhedsniveau

Det kan være en barriere for en virksomheds IT-sikkerhed, hvis medarbejderne og ledelsen ikke har tilstrækkelig viden om IT-sikkerhed. Det kan dog også være en barriere, at den IT-ansvarlige ikke har tilstrækkelig viden om trusselsbilledet samt de produkter og løsninger, der er på markedet. Hvis den IT-ansvarlige ikke har denne viden, er arbejdet med IT-sikkerhed svært, men det kan også betyde, at virksomheden ikke vurderer sin IT-sikkerhed på et tilstrækkeligt videngrundlag. Det kan medføre, at virksomhederne ser deres IT-sikkerhed som tilstrækkelig, fordi de ikke ved, hvordan trusselsbilledet ser ud og ændrer sig.

En for lav grad af information kan være en barriere, men overvægt af information kan også være en udfordring, fordi det kan være svært at navigere i de informationer og produkter, der er på markedet, og det kan i særlig grad være svært at vurdere, hvad der er relevant for ens egen virksomhed. To af virksomhederne påpeger, at der er en meget stor informationsmængde, og at det kan være svært at navigere heri og vurdere, hvad der er nødvendigt for deres virksomhed, og hvad der er mindre vigtigt. Da informationsmængden er stor og forskelligartet, er det svært at trække essensen ud og koge det ned til noget, man kan bruge i virksomheden. Omvendt ser fem af virksomhederne det som en drivkraft for deres IT-sikkerhed, at de føler sig tilstrækkelig informeret om IT-sikkerhed. Det er videnniveauet, der gør virksomheden i stand til at agere på de IT-sikkerhedstrusler, der er, og det fungerer dermed som virksomhedens radar. Det bliver derfor klart, at viden er en central faktor for at kunne vurdere sit eget sikkerhedsniveau, og denne viden kan virksomhederne få fra forskellige kilder.

Halvdelen af de adspurgte virksomheder får en stor del af deres viden fra eksterne samarbejdspartnere og leverandører. Af kapitel 4 fremgik det, at 72 procent af de danske SMV'er samarbejder med en ekstern rådgiver/samarbejdspartner om IT-sikkerhed. Dette understreger, at man ofte har et samarbejde med en ekstern aktør, som kan bruges til at opnå viden om IT-sikkerhed. Udover at anvende eksterne samarbejdspartnere til at opnå viden om IT-trusler og -sikkerhed er der også virksomheder, der anvender forskellige netværk som informationskilde(r) både af privat og offentlig karakter.

5.3.1 En kilde til viden til IT-sikkerhed er professionelle og personlige netværk

Fem af virksomhederne nævner, at de bruger deres professionelle og personlige netværk til at opnå information om IT-sikkerhed og ikke mindst dele erfaringer og sparre om IT-sikkerhed, og at disse netværk derfor bliver en drivkraft for deres IT-sikkerhed, fordi de giver dem adgang til viden. I Sørensen Produktion oplever man, at erfaringsdeling med virksomheder i ens netværk er vigtig, og at det kan være givende at høre, hvordan andre har håndteret specifikke udfordringer, herunder hvis andre virksomheder har haft et sikkerhedsbrud. I TP Aerospace er det helt essentielt for den IT-ansvarlige at erfaringsdele i sit netværk. Denne sparring vurderes som særlig værdifuld, når man skal vurdere, hvilke tiltag der er relevante for virksomheden, fordi det kan være en jungle at navigere i IT-sikkerhed på egen hånd.

ToBu Transport er en del af to branchefora, hvor man deler erfaring og viden indenfor IT-sikkerhed, og man har derudover kørt nogle forskellige test sammen. Det beskrives i Case 7, hvordan disse fora er særlig værdifulde, fordi de giver mulighed for at sparre med sammenlignelige virksomheder.

ToBu Transport om brugen af fora vedrørende IT-sikkerhed

Navn | ToBu Transport

Branche | Transport

Størrelse | 100 medarbejdere

IT-sikkerhedsniveau | Høj

Risikoprofil | Middel

ToBu Transport er et transportselskab, der primært henvender sig til private.

ToBu Transport er en del af to branchefora vedrørende IT-sikkerhed. ToBu Transport ser stor værdi i at deltage i disse fora, da de kan dele erfaringer med lignende virksomheder, der står overfor de samme udfordringer, som de selv gør, og sparre om nye produkter og tilbud. Det betyder, at de oplever, at de er mere opdaterede og derfor har mere relevant viden om IT-sikkerhed, hvilket gør dem i stand til at opnå et tilstrækkeligt højt IT-sikkerhedsniveau.

Man har i samarbejde med andre medlemmer også kørt en test, hvor man testede IT-sikkerheden af virksomhedernes betalingssystemer – en test, som virksomheden ikke mente, den ville være i stand til at lave, hvis den skulle lave testen på egen hånd.

Case 7. ToBu Transport

Udover brancherelaterede fora findes der også andre tværgående fora. I Aarhus Teater og TP Aerospace er man medlem af Rigspolitiets NC3Skyt, som er et samarbejde mellem virksomheder og politi, hvorigennem man deler erfaringer og får information om, hvad der rører sig i forhold til IT-sikkerhed. Virksomhederne efterspørger, at der samarbejdes mere på tværs af virksomheder og politi, og at der i højere grad udveksles oplysninger og erfaringer for samlet at øge IT-sikkerhedsniveauet.

Udover at anvende formelle, professionelle fora opsøger de IT-ansvarlige i mange af virksomhederne også selv information i forskellige fora på nettet, fordi de har en personlig interesse i IT-sikkerhed og ønsker at holde sig opdateret på området. I casevirksomheden FinansieringNu ser man som en del af opgaven som IT-ansvarlig at holde sig opdateret på IT-sikkerhed, men man har samtidig også stor interesse for området og forsøger at holde sig opdateret.

5.4 En høj risikoprofil er en drivkraft for en øget IT-sikkerhed i virksomhederne

Hvis en virksomhed oplever et IT-sikkerhedsbrud, kan det ramme virksomheden på en lang række måder. Udover at medføre direkte omkostninger til at løse problemet kan det betyde, at virksomhedens medarbejdere ikke kan arbejde, eller at driften på anden vis afbrydes. For 10 af de interviewede virksomheder er arbejdet med IT-sikkerhed derfor drevet af et ønske om at undgå IT-nedbrud. Dette er især tilfældet for virksomheder, hvor man har identificeret, at man har nogle meget kritiske systemer, som forretningen ikke kan fungere uden. Drivkraften for arbejdet med IT-sikkerhed er derfor relateret til virksomhedens risikoprofil. Da mange virksomheder samtidig ser, at IT-trusselsbilledet øges, øges bekymringen for et IT-sikkerhedsbrud, og man ønsker at være proaktiv for at undgå dette, og dermed bliver IT-trusselsbilledet også en drivkraft. Dermed gælder bekymringen både de konsekvenser, et IT-sikkerhedsbrud kan have, men også den øgede risiko for et IT-sikkerhedsbrud som følge af et højere IT-trusselsbillede.

Udover at et nedbrud kan betyde, at virksomhedens medarbejdere ikke kan udføre deres arbejde, kan det også påvirke virksomhedens image overfor kunderne, fordi de ikke er i stand til at servicere dem på en tilstrækkelig måde. Det er blandt andet tilfældet i Blå Maritim, hvor man ønsker, at ens systemer er sikre, så man kan opnå en høj driftssikkerhed. Man har vurderet, at virksomhedens systemer er særlig kritiske for forretningen, og den høje afhængighed af IT-systemer og data betyder derfor, at man ønsker, at IT-sikkerheden er tilsvarende høj. For Blå Maritim hænger det derudover også tæt sammen med det image, man ønsker at opretholde overfor kunderne, der vil lide overlast, hvis virksomheden ikke kan opretholde driften.

I Sund & Bælt har man ligesom i Blå Maritim identificeret, at der er en række systemer, der er meget kritiske for forretningen og virksomhedens drift, som det beskrives i Case 8.

Sund & Bælt om, hvordan sikring af driften er en drivkraft for arbejdet med IT-sikkerhed

Navn | Sund & Bælt

Branche | Transport

Størrelse | 127 medarbejdere

IT-sikkerhedsniveau | Høj

Risikoprofil | Middel

Sund & Bælt er et holdingselskab, der ejer aktier i og forestår den overordnede styring af datterselskaberne.

Sund & Bælt foretager årligt en risikovurdering, hvor de kortlægger alle systemer og identificerer de centrale arbejdsprocesser. Denne risikovurdering har identificeret en række systemer, der er meget kritiske for forretningen, og Sund & Bælt har vurderet, at medarbejderne ikke vil kunne arbejde, hvis disse systemer angribes, hvilket vil være forretningskritisk. Virksomheden ønsker derfor at have en høj IT-sikkerhed, så den blandt andet også undgår, at medarbejderne ikke kan udføre deres arbejde i en periode, og de har således vurderet, hvad der skal til for at håndtere risici relateret til disse systemer.

Endvidere forventer Sund & Bælt, at de i fremtiden vil blive mere datadrevet i deres arbejde, og at data, i takt med at IT bliver mere kompleks, bliver en mere central del af forretningen. Virksomheden ønsker derfor at bringe IT-sikkerhed ind fra starten for at sikre disse data i tilstrækkelig grad og derudover på forhånd øge fokus på IT-sikkerhed internt.

Case 8. Sund & Bælt

Frygten for et IT-sikkerhedsbrud kan betyde, at man vælger at indføre mere IT-sikkerhed, men man kan også opleve et egentligt IT-sikkerhedsbrud, der kan betyde, at virksomheden oplever konsekvenserne ved et IT-sikkerhedsbrud. Dette kan få virksomhederne til reaktivt at indføre mere IT-sikkerhed for at undgå fremtidige sikkerhedsbrud, hvilket beskrives i næste afsnit.

5.4.1 Et IT-sikkerhedsbrud øger virksomhedens forståelse for deres risikoprofil og øger fokus på IT-sikkerhed

Hvis man som virksomhed oplever et IT-sikkerhedsbrud, kan det blive en drivkraft for arbejdet med at øge IT-sikkerheden, fordi man oplever, hvor kritisk et sikkerhedsbrud kan være. 35 procent af virksomhederne i caseinterviewene har oplevet et IT-sikkerhedsbrud i større eller mindre grad og oplevede, at dette blev en drivkraft for deres arbejde med IT-sikkerhed. Det betød, at de udover at øge deres IT-sikkerhedsforanstaltninger også kunne bruge IT-sikkerhedsbruddet i kommunikationen internt til både ledelsen og medarbejderne. Som beskrevet i Case 4 i kapitel 4 oplevede Danmarks Naturfredningsforening for over 10 år siden et systemnedbrud, hvor de mistede mange data, som de ikke havde backup af. Det betød, at der kom øget fokus på og forståelse af IT-sikkerhed, og at man iværksatte flere tiltag, herunder backup, for ikke at risikere, at det samme skulle ske igen. Det medvirkede til, at IT-sikkerheden blev mere håndgribelig, og at medarbejderne kunne se IT-sikkerhed i sammenhæng med deres arbejde. Da man senere oplevede et ransomwareangreb, var de negative konsekvenser derfor begrænsede, da man kunne anvende sin backup til at genskabe data. I Case 9 beskrives det, hvordan Aarhus Teater oplevede et sikkerhedsbrud, og hvordan det fik stor betydning for driften af virksomheden. Udover at det fik negative konsekvenser for virksomheden, betød det dog også, at der kom en større forståelse af IT-sikkerhed blandt medarbejderne.

Aarhus Teater om, hvordan et IT-sikkerhedsbrud blev en drivkraft for arbejdet med IT-sikkerhed

Navn | Aarhus Teater

Branche | Kultur, forlystelser og sport

Størrelse | 100-249 medarbejdere

IT-sikkerhedsniveau | Middel

Risikoprofil | Middel

Aarhus Teater opfører teaterforestillinger i den midtjyske region.

I februar 2017 oplevede Aarhus Teater et IT-sikkerhedsbrud, hvor de opdagede, at deres filer var i gang med at blive krypteret, fordi en medarbejder utilsigtet var kommet til at trykke på et link og på den måde lukke ransomware ind i Aarhus Teaters IT-systemer. IT-sikkerhedsbruddet blev stoppet ved at lokalisere kilden, men inden da var 11.000 af virksomhedens 300.000 filer blev krypteret, hvilket betød, at virksomheden ikke kunne bruge IT i fire dage. Umiddelbart er der efterfølgende ingen langvarige konsekvenser, og ingen medarbejdere har aktivt givet udtryk for, at der var filer, der gik tabt.

Bruddet påvirkede naturligvis teatret i den tid, IT var nede, men det betød også, at der kom større fokus på IT-sikkerhed internt i virksomheden. Det blev klart for både medarbejdere og ledelse, hvad manglende IT-sikkerhed kunne betyde, og det blev meget håndgribeligt og forståeligt, hvilke konsekvenser et IT-sikkerhedsbrud kunne få. Det lettede dermed også den fremadrettede kommunikation til medarbejderne og ledelsen, da de havde en større forståelse af betydningen af IT-sikkerhed.

Case 9. Aarhus Teater

5.5 Outsourcingpartnere øger IT-sikkerhedsniveauet, men introducerer eksterne risici

Som vi så i kapitel 4, har en stor del af de danske SMV'er outsourcet hele eller dele af deres IT til en ekstern leverandør. Når virksomheden vælger at gøre dette, bliver den afhængig af leverandøren. Leverandøren bliver således vigtig for IT-sikkerheden, men virksomheden får samtidig adgang til flere kompetencer, hvilket kan være med til at øge IT-sikkerheden, i forhold til hvis denne skulle håndteres internt. Som det også fremgik af kapitel 4, havde virksomheder, der havde outsourcet IT, generelt et højere IT-sikkerhedsniveau, hvilket indikerer, at outsourcing kan være en måde at øge IT-sikkerheden på.

10 af virksomhederne i caseinterviewene har valgt at outsource hele eller dele af deres IT, hvilket betyder, at deres leverandør i høj grad bliver en vigtig faktor i og drivkraft for virksomhedens IT-sikkerhed. Alle disse virksomheder opfatter dette som en drivkraft for deres IT-sikkerhed, fordi de får adgang til flere kompetencer, og fordi deres IT-sikkerhed varetages af nogle, der har IT-spidskompetencer. FinansieringNu har outsourcet dele af deres IT, og de vurderer, at fordi de er en lille virksomhed, kan de ikke være 100 procent gode til alt. De ser dog, at 80 procent ikke er nok, når det kommer til IT-sikkerhed, og derfor har de valgt at gøre brug af outsourcing, så de overlader det til nogen, der besidder de nødvendige kompetencer. Casevirksomheden Graf Design påpeger, at fordi de har outsourcet hele deres IT til en ekstern leverandør, bliver leverandøren instrumentel for virksomhedens IT-sikkerhed. Virksomheden oplever, at dette øger deres IT-sikkerhed, fordi de ikke selv har de nødvendige kompetencer til at varetage IT-sikkerheden, og at de får adgang til flere kompetencer ved at bruge en ekstern leverandør.

I Graf Design italesætter man også, at dette betyder, at man fuldstændig sætter sin lid til den eksterne leverandør, og at det kræver en høj grad af tillid. Dette anerkender man også i Sørensen Produktion, og i Case 10 beskrives det, hvordan Sørensen Produktion har outsourcet IT, og hvordan de vurderer, det påvirker deres IT-sikkerhed.

Sørensen Produktion om outsourcings betydning for IT-sikkerheden

Navn | Sørensen Produktion

Branche | Industri

Størrelse | 10-19 medarbejdere

IT-sikkerhedsniveau | Middel

Risikoprofil | Middel

Virksomheden producerer trævarer og genanvender blandt andet træ.

Sørensen Produktion har outsourcet hele deres IT til en ekstern samarbejdspartner, fordi de vurderer, at de ikke har de nødvendige kompetencer internt og derfor ser, at det løfter deres IT-sikkerhed at bruge en outsourcingpartner. De anerkender dog også, at de er fuldstændig afhængige af denne leverandør i forhold til deres IT-sikkerhed. De ser det derfor også som en udfordring, at de ikke selv har den nødvendige viden og de nødvendige kompetencer til at kunne udfordre leverandøren på og stille krav til dennes IT-sikkerhed.

Sørensen Produktion har oplevet konsekvensen af, at de ikke selv i tilstrækkelig grad var i stand til at udfordre deres leverandør på IT-sikkerhed. Man oplevede, at en leverandør mistede en del af virksomhedens data, fordi leverandøren ikke havde foretaget tilstrækkelig eller korrekt databackup, og man valgte derfor at skifte til en anden leverandør. I virksomhedens søgen efter en ny leverandør var der derfor også øget fokus på IT-sikkerhed. Man brugte i høj grad referencer fra netværket til at finde en ny leverandør.

Case 10. Sørensen Produktion

Ud fra case 10 er det klart, at man som virksomhed bør stille krav til sin leverandør vedrørende IT-sikkerhed, fordi leverandøren bliver afgørende for, at ens systemer og data er sikre. Man bør blandt andet stille krav til databehandling, backup, opdatering af systemer og andre IT-sikkerhedsforanstaltninger. Har man valgt at outsource sin IT, er det vigtigt, at man stadig tager ansvar for sin IT-sikkerhed, selvom det kan være udfordrende at stille de nødvendige krav, fordi det kræver, at man tilegner sig viden og holder sig opdateret. Derudover bør man have en databehandleraftale. Som det fremgik i kapitel 4, er det imidlertid kun 53 procent af de virksomheder, der har outsourcet hele deres IT, der har en databehandleraftale, og kun 39 procent af de virksomheder, der har outsourcet dele af deres IT, der har en databehandleraftale. I DST VITA fra 2016 stiller 42 procent af virksomhederne krav til deres leverandører vedrørende IT-sikkerhed, hvilket bekræfter, at der er en stor andel, der ikke forholder sig til sine leverandørers IT-sikkerhed. Dette tal burde være højere, fordi leverandørerne kan opbevare data, for eksempel om virksomhedens produkter, der kan være kritiske for ens virksomhed, og fordi man ikke selv har kontrol over, hvordan disse data håndteres.

5.6 Prioritering af ressourcer kan udskyde IT-sikkerhedstiltag

Alle virksomheder er nødt til at prioritere deres ressourcer, da de har begrænsede ressourcer til rådighed, hvilket kan blive en barriere for arbejdet med IT-sikkerhed. Som med andre typer opgaver kan man som virksomhed være nødt til at udskyde en opgave eller et tiltag, fordi man ikke har de nødvendige ressourcer til rådighed på det tidspunkt, man skal bruge dem. 10 af virksomhederne i caseinterviewene oplever, at dette har været tilfældet i forbindelse med opgaver relateret til IT-sikkerhed, men at det generelt handler om, at man udskyder opgaven til et senere tidspunkt – ikke, at man helt vælger at droppe opgaven. Her er der enkelte af virksomhederne, der vælger at bruge eksterne konsulenter til at løse opgaven, men der er også virksomheder, der fravælger det, fordi de ønsker at opbygge viden og kompetencer internt, så de er i stand til også at varetage opgaven i fremtiden.

Udover at man skal prioritere sine ressourcer i forhold til andre opgaver, skal man prioritere sin indsats i forhold til IT-sikkerhed og vurdere, hvor højt et IT-sikkerhedsniveau man behøver. For nogle virksomheder handler det derfor i høj grad også om at vurdere risikoprofilen i forhold til behovet for IT-sikkerhed, så man ikke overimplementerer tiltag og får en højere IT-sikkerhed end nødvendig. Aarhus Teater forsøger at finde denne balance, da de vurderer, at de aldrig kan være sikret 100 procent mod IT-sikkerhedsbrud, og det handler derfor om at finde det IT-sikkerhedsniveau, der passer til ens virksomhed. Det samme gælder for Maskinhandler Indkøbsringen, der også anerkender, at man kan implementere så meget IT-sikkerhed, at det vil forstyrre driften og medarbejdernes arbej-

de. Man skal derfor finde det niveau, der sikrer ens IT-sikkerhed, og som samtidig gør det muligt at drive forretningen, og som er forenelig med virksomhedens risikovurdering og risikoappetit.

5.7 IT-sikkerhed giver på nuværende tidspunkt kun begrænset kommerciel differentiering

Da man som virksomhed i visse tilfælde også håndterer kritiske eller følsomme data for sine kunder, kunne man antage, at kunderne efterspurgte et højt niveau af IT-sikkerhed og ansvarlig datahåndtering og måske endda stillede det som et krav for et eventuelt samarbejde. Det er dog kun AB Hjem, der i enkelte tilfælde har oplevet, at deres udenlandske privatkunder har spurgt til sikkerheden på virksomhedens hjemmeside og samtidig til adgangskodeopsætningen på deres hjemmeside. I stedet for at afvente, at kunderne efterspørger IT-sikkerhed, kan man som virksomhed selv bruge det aktivt i forhold til kunderne. Det er dog kun casevirksomheden Secure Service, der aktivt bruger deres IT-sikkerhed i kommunikationen til deres kunder, som det beskrives i Case 11.

Secure Service om konkurrencemæssig differentiering som en drivkraft for IT-sikkerhed

Navn | Secure Service

Branche | Serviceydelser

Størrelse | 50-99 medarbejdere

IT-sikkerhedsniveau | Høj

Risikoprofil | Høj

Secure Service sælger IT-løsninger til andre virksomheder.

Secure Service er en virksomhed, der varetager IT for andre virksomheder, og de ser derfor IT-sikkerhed som en helt central del af deres forretning. Secure Service bruger også deres arbejde med IT-sikkerhed aktivt som en salgsparameter overfor deres kunder, da de ser, det kan være en differentierende faktor i forhold til deres konkurrenter. Secure Service får udarbejdet en 3420-erklæring, hvor de bliver revideret på deres IT-sikkerheder. Resultaterne af denne sender de ud til deres kunder for at vise, hvad de er blevet revideret på, og hvor der er huller. Secure Service ser IT-sikkerhed som en stor del af deres image, og de ønsker derfor at dele de revisioner, de får foretaget, og de forklarer samtidig, hvilke tiltag de foretager på området – både for at imødekomme resultaterne fra revisionen og nye tiltag. Hos Secure Service håber man også, at sidstnævnte kan bruges til at inspirere kunderne til lignende tiltag i deres virksomheder, og at Secure Service på den måde kan være med til at løfte IT-sikkerhedsniveauet på tværs.

Case 11. Secure Service

Det er således en lille andel af virksomhederne, der på nuværende tidspunkt oplever, at deres kunder spørger ind til IT-sikkerhed, men flere af virksomhederne forventer, at deres kunder vil stille krav til IT-sikkerhed i fremtiden. Dette gælder for Fremtidens Læring, der forventer, at deres kunder i fremtiden vil stille krav til, hvordan virksomheden håndterer deres data. Det samme gør sig gældende i Danmarks Naturfredningsforening, og man vurderer, at dette sandsynligvis vil blive drevet af et større sikkerhedsbrud, som bliver omtalt i medierne, hvor en virksomhed eller forening får lækket en lang række følsomme personoplysninger.

5.8 Lovgivning er en drivkraft for øget IT-sikkerhed, men kræver mange ressourcer af virksomhederne

Udover at kunderne kan være en ekstern drivkraft for en virksomheds IT-sikkerhed, kan lovgivning også være en ekstern drivkraft for virksomhedernes arbejde med IT-sikkerhed. For visse brancher gælder der særlig lovgivning, der stiller krav til virksomhedens IT-sikkerhed, og for fire af de adspurgte virksomheder er lovgivning en drivkraft for deres arbejde med IT-sikkerhed. Sund & Bælt er underlagt IT-revision, og derfor arbejder man i virksomheden med at lukke de eventuelle huller, som disse revisioner afdækker. I TP Aerospaces branche er det påkrævet, at man har en række certificeringer, for at man må drive forretning, og når man skal igennem auditeringer for at beholde disse certificeringer, oplever man, at disse auditeringer går lettere, fordi virksomheden har øget IT-sikkerheden.

Med den kommende persondataforordning vil alle virksomheder, der behandler persondata, blive påvirket af lovgivningen, og der er da også tre af virksomhederne, der nævner, at persondataforordningen har haft en betydning for deres arbejde med IT-sikkerhed. I Sund & Bælt har det krævet en øget indsats i forhold til at afdække, hvilke data virksomheden besidder, og i hvilken grad virksomheden har brug for disse data. Det samme gør sig gældende

for AB Hjem, hvor man vurderer, at persondataforordningen ikke bare vil betyde, at man skal have større fokus på IT-sikkerhed fremadrettet, men også at det vil få betydning for hele organisationens arbejdsprocesser. I Secure Service har persondataforordningen også haft stor betydning, da det har betydet, at ledelsen er blevet mere opmærksom på IT-sikkerhed. Ikke kun, fordi man risikerer at få en stor bøde, hvis man ikke lever op til denne, men i høj grad også, fordi det kan medføre et imagetab, hvis man bliver involveret i en retssag, fordi man ikke lever op til persondataforordningen.

Persondataforordningen er dog en kompleks størrelse, og Maskinhandler Indkøbsringen forklarer, at udover at være presset på tid til at sætte sig ind i tingene, er det også meget svært at forstår, hvad det kræver at leve op til forordningen. Da Maskinhandler Indkøbsringen er en mindre virksomhed, har den ikke ressourcer til blot at ansætte en til at håndtere det, som de forventer, større virksomheder vil have. Maskinhandler Indkøbsringen er derfor afhængig af input udefra. De oplever dog, at deres brancheforening ikke er i stand til at vejlede, og at de heller ikke kan søge input fra offentlige myndigheder. Persondataforordningen ses som en drivkraft for at arbejde med IT-sikkerhed og databeskyttelse, men Maskinhandler Indkøbsringen ser også, at den bliver en bremse for andre IT-sikkerhedsrelaterede tiltag, fordi de nu og her er nødt til at bruge mange ressourcer på at leve op til persondataforordningens krav.

5.9 Opsummering

Kapitel 5 har afdækket, hvilke barrierer og drivkræfter danske SMV'er oplever i deres arbejde med IT-sikkerhed.

Medarbejdernes handlinger og manglende viden er en af de første barrierer, som virksomhederne nævner i forbindelse med IT-sikkerhed. Medarbejdernes handlinger og manglende viden skaber udfordringer for arbejdet med IT-sikkerhed, hvilket virksomhederne overkommer ved kontinuerligt at kommunikere IT-sikkerhedstrusler og potentielle konsekvenser ved et IT-sikkerhedsbrud. Generelt oplever virksomhederne, at det er centralt at forankre IT-sikkerhed i virksomhedskulturen for at opnå et tilstrækkeligt fokus og en tilstrækkelig opmærksomhed. Ledelsens manglende engagement i IT-sikkerhed er ligeledes en barriere for IT-sikkerhed, fordi ledelsen skal allokere de nødvendige ressourcer, og de spiller samtidig en central rolle i at skabe virksomhedskulturen. Virksomhederne oplever, at det manglende engagement typisk er forårsaget af, at ledelsens fokus i højere grad ligger på det kommercielle, og at de derudover ikke besidder tilstrækkelig viden omkring IT-sikkerhed eller kan se koblingen mellem IT-sikkerhed og forretningen. En måde at øge ledelsens engagement på er derfor at øge dens videnniveau, ligesom hos medarbejderne, ved at kommunikere IT-sikkerhed til ledelsen. Flere af virksomhederne benytter sig i denne forbindelse af eksterne risikoanalyser og -test i deres kommunikation, hvilket blandt andet medfører, at IT-sikkerhed bliver mere håndgribelig og forståelig.

Udover medarbejdernes og ledelsens niveau af viden om IT-sikkerhed er det også centralt, at de IT-ansvarlige i virksomhederne har et tilstrækkeligt videnniveau om IT-sikkerhed, da dette er definerende for virksomhedens IT-sikkerhed. Videnniveauet er afgørende for, at virksomheden ved, hvilke trusler der er, og hvilke løsninger der er på markedet, og derfor hvilket IT-sikkerhedsniveau der er tilstrækkeligt. Udover at få denne viden fra samarbejdspartnere, for eksempel en outsourcingpartner, får virksomhederne i høj grad deres viden fra deres professionelle såvel som personlige netværk.

For nogle af virksomhederne er en drivkraft for deres arbejde med IT-sikkerhed, at de ser, de har en høj risikoprofil, og at de derfor er nødt til at have et højt IT-sikkerhedsniveau for at undgå et IT-nedbrud. Samtidig ser virksomhederne, at der er et øget IT-trusselsbillede, hvilket øger risikoen for et IT-sikkerhedsangreb, hvilket får dem til at øge IT-sikkerheden yderligere. Nogle af virksomhederne har oplevet et egentligt IT-sikkerhedsbrud, hvilket har gjort, at de har fået en større forståelse for de konsekvenser, et IT-sikkerhedsbrud kan have, og de vælger derfor at øge fokus på IT-sikkerhed. Dette øgede fokus er ikke kun blandt virksomhedens IT-ansvarlige, men også virksomhedens øvrige ledelse og medarbejdere.

En stor del af danske SMV'er har outsourcet hele eller dele af deres IT, og i disse tilfælde er deres outsourcingpartner afgørende for virksomhedens IT-sikkerhed. Virksomhederne oplever dog, at det øger deres IT-sikkerhed, at de anvender en outsourcingpartner, fordi de får adgang til kompetencer, de ikke besidder internt. Det betyder dog også, at man som virksomhed har svært ved at udfordre outsourcingpartneren på IT-sikkerhed, fordi man ikke besidder de rigtige kompetencer. Hvis virksomheden skal sikre, at de har et tilstrækkeligt IT-sikkerhedsniveau, er virksomheden derfor nødt til at have viden på området, så den bliver i stand til at stille krav til deres outsourcingpartner og leverandører generelt.

For nogle af virksomhederne gælder der særlig lovgivning, som derfor bliver en drivkraft for deres arbejde med IT-sikkerhed, og der er også flere af virksomhederne, som nævner persondataforordningen som en drivkraft for deres

arbejde med IT-sikkerhed. Dog kræver det mange ressourcer at leve op til persondataforordningen, og det kan derfor få betydning for arbejdet med andre områder af IT-sikkerhed.

6 Negative og positive konsekvenser ved IT-sikkerhed

Danske SMV'er oplever konsekvensen af manglende IT-sikkerhed, og selvom det er svært at estimere antallet af IT-sikkerhedshændelser, har omtrent hver syvende SMV, ifølge indeværende analyse, oplevet et IT-sikkerhedsbrud. IT-sikkerhedsbruddene kan være omfattende for virksomhederne både i form af direkte omkostninger og tabte kommercielle muligheder. IT-sikkerhed ses endnu ikke som en konkurrenceparameter for danske SMV'er, og flere virksomheder peger på, at myndighederne bør tage en større rolle i at drive IT-sikkerhed i Danmark.

Dette kapitel går i dybden med konsekvenserne af utilstrækkelig IT-sikkerhed og ser også på IT-sikkerhed som en konkurrenceparameter i danske virksomheder. Endelig beskrives det i kapitlet, hvordan virksomhederne og udvalgte eksperter ser myndighedernes rolle i udviklingen af IT-sikkerhed.

6.1 Konsekvenser ved manglende IT-sikkerhed kan være omfattende for en virksomhed

Det er generelt svært at estimere, hvor mange virksomheder der har haft et IT-sikkerhedsbrud. Det skyldes, at det ikke er alle virksomheder, der ønsker at oplyse om IT-sikkerhedsbrud, som det også blev beskrevet i kapitel 3 omkring mørketal. I denne undersøgelse har cirka hver syvende danske SMV på et tidspunkt oplevet et IT-sikkerhedsbrud, og hvis man skalerer dette op til hele populationen, svarer det til, at 11.000 danske SMV'er har oplevet et IT-sikkerhedsbrud.

Et IT-sikkerhedsbrud kan have store konsekvenser for en virksomhed, og som beskrevet i case 9 oplevede Aarhus Teater konsekvenserne af et IT-sikkerhedsbrud. Oplever en virksomhed et IT-sikkerhedsbrud kan det have økonomiske konsekvenser enten som omkostninger som direkte følge af bruddet eller som indirekte omkostninger. De direkte omkostninger er kortsigtede og derfor nemmere at estimere, da de typisk opstår i forbindelse med IT-sikkerhedsbruddet, mens de indirekte omkostninger er langsigtede og derfor mere usikre at estimere. 6 procent af SMV'erne i denne undersøgelse svarer, at de har oplevet et IT-sikkerhedsbrud indenfor det sidste år. Af disse havde 74 procent omkostninger relateret til IT-sikkerhedsbruddet vurderet til 36.000 kr. i gennemsnit. For flere end hver 10. estimeredes omkostningerne dog væsentligt højere og lå mellem 100.000 og 200.000 kr.

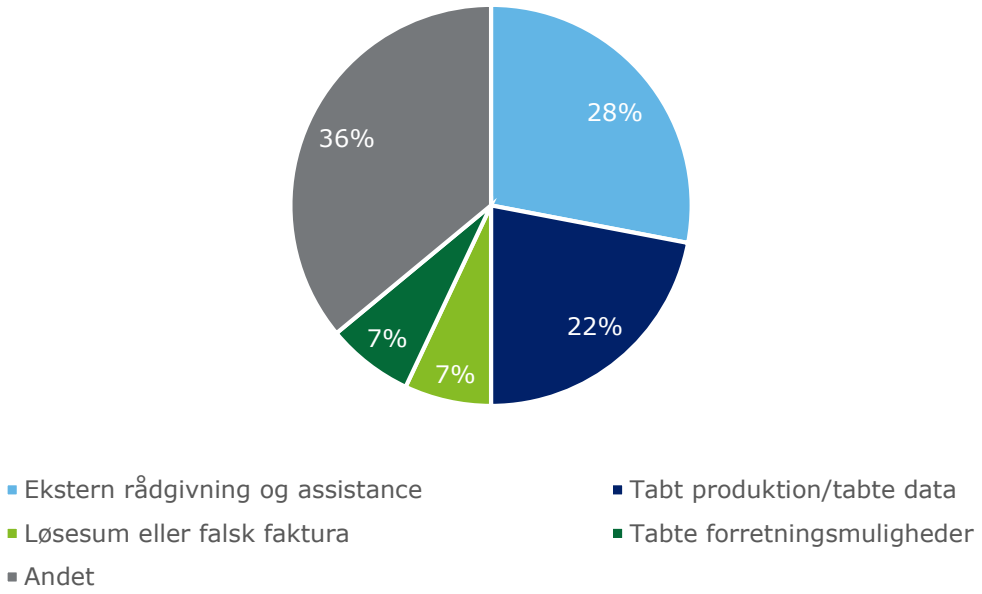
Direkte og indirekte omkostninger ved et IT-sikkerhedsbrud

Der skelnes mellem to forskellige typer omkostninger forbundet med IT-sikkerhedsbrud.

Direkte omkostninger er relateret direkte til IT-sikkerhedsbruddet og dækker blandt andet rådgivning, brug af eksterne ressourcer til at udbedre problemet samt gendannelse af data. De direkte omkostninger har typisk et kortsigtet perspektiv.

Indirekte omkostninger er mere langsigtede følgevirkninger af IT-sikkerhedsbruddet og dækker blandt andet forringet image, mistede forretningskritiske data, tabte kommercielle muligheder og som følge heraf tabt omsætning.

Figur 32. SMV'ernes omkostninger i forbindelse med et IT-sikkerhedsbrud



Kilde: Wilke for Monitor Deloitte

Som det fremgår af Figur 32, dækkede omkostningerne for 28 procent af de ramte virksomheder udgifter til ekstern rådgivning og assistance, mens de i 22 procent af tilfældene dækkede tabt produktion/tabte data. Syv procent mistede direkte penge til betaling af løsesum i forbindelse med ransomware eller betaling af falske fakturaer, mens syv procent mistede forretningsmuligheder som direkte følge af IT-sikkerhedsbruddet.[11]

De 36.000 kr., som denne analyse fandt frem til, at et IT-sikkerhedsbrud i gennemsnit koster, virker dog generelt som et lavt tal, når der sammenlignes med andre undersøgelser. En årsag hertil kan være, at virksomhederne i indeværende undersøgelse primært tænker på de direkte omkostninger forbundet med IT-sikkerhedsbruddet. Tallet virker lavt, hvis man for eksempel sammenligner med PwC's undersøgelse, hvor de økonomiske konsekvenser opgøres til 900.000 kr.[12]. IT-sikkerhedsfirmaet Kaspersky har lavet en undersøgelse af industri- og forsyningsvirksomheder, hvor omkostningerne beregnes til årligt at løbe op i 3,3 mio. kr.[13]

Omkostningerne til et IT-sikkerhedsbrud er som nævnt ikke begrænset til omkostninger direkte relaterede til IT-sikkerhedsbruddet, men kan også være indirekte omkostninger. De indirekte omkostninger kan være relateret til, at medarbejderne ikke kan udføre deres arbejde, og disse omkostninger kan ikke estimeres lige så præcist som ovenstående, men de kan have stor betydning for virksomhederne. Flere cases beskrevet i kapitel 5 omtaler, hvordan det var en drivkraft at undgå IT-nedbrud, fordi virksomhedernes medarbejdere derved ikke ville være i stand til at udføre deres arbejde. Effekten af et IT-sikkerhedsbrud vil variere alt afhængig af varigheden af nedbruddet. En rapport fra Cisco fra 2017, der indeholder en omfattende afdækning af IT-sikkerhed på tværs af flere lande, beskriver, hvordan næsten hver 10. virksomhed, der oplever et IT-sikkerhedsbrud, har nedbrud i systemerne i mere end 24 timer. Det er derimod kun 7 procent, der ikke oplever, at deres systemer er nede som følge af et IT-sikkerhedsbrud[14]. Hvis man som 69 procent af de danske SMV'er i høj grad har systemer, der er kritiske for ens

[11] Wilke for Monitor Deloitte

[12] https://www.pwc.dk/da/nyt/publikationer/cybercrime-survey-2017.html

[13]https://finans.dk/tech/ECE9716814/taber-millioner-paa-hacking-industrivirksomheder-har-alvorlige-brud-paa-itsikkerheden/?ctxref=ext

[14] Cisco, Annual Cybersecurity Rapport, 2017.

forretning, kan det derfor have store konsekvenser for en virksomhed, hvis systemerne er nede i 24 timer. Det vil betyde, at virksomhedens medarbejdere ikke kan arbejde, hvilket blandt andet kan medføre, at den ikke kan servicere sine kunder eller modtage nye ordrer, hvilket kan medføre tab af forretningsmuligheder.

For nogle virksomheder kan omkostningerne være mere omfattende og langsigtede end tabt arbejde, da indeværende undersøgelse peger på, at 16 procent af danske SMV'er kan miste deres forretningsgrundlag, hvis deres forretningskritiske data bliver lækket. Det kan eksempelvis være virksomheder, der opbevarer intellektuel ejendom og fortrolige informationer om deres kunder. For disse virksomheder vil et IT-sikkerhedsbrud for alvor true virksomhedens eksistens, og omkostningerne kan være umulige at estimere, da de ofte relaterer sig til tab af forretningsmuligheder, man endnu ikke har opnået.

De langsigtede omkostninger kan blandt andet også relatere sig til tabt omsætning og forringelse af image. I rapporten fra Cisco har 29 procent af de adspurgte virksomheder oplevet et omsætningstab som følge af et IT-sikkerhedsangreb; af de 29 procent mistede 38 procent betydelig omsætning[15]. I caseinterviewene beskrev flere virksomheder, hvordan et IT-sikkerhedsbrud kunne påvirke deres image overfor kunderne, hvilket kan medføre, at de mister kommercielle muligheder. Denne bekymring er berettiget, for som Cisco beskriver i deres rapport, var der 22 procent af de adspurgte, der havde mistet kunder som følge af et IT-sikkerhedsbrud, hvoraf næsten 40 procent mistede en femtedel af deres kunder eller derover.[16]

Afhængigt af IT-sikkerhedsbruddets karakter kan det også få betydning for virksomhedens konkurrencefordel, hvis der er tale om erhvervsspionage. I modsætning til ransomware, hvor bagmanden ofte ønsker hurtigt at kryptere alle virksomhedens data for at få udbetalt en løsesum, vil man ved erhvervsspionage typisk se, at hackeren forsøger at komme uset ind i systemerne og hente forretningskritiske data, uden det opdages. Herved opnår bagmanden adgang til forretningskritiske data som eksempelvis intellektuel ejendom, som bagmanden kan anvende enten som afpresning eller sælge videre til konkurrenter. Ifølge Verizons rapport om IT-sikkerhedsbrud er motivet bag cirka en fjerdedel af alle IT-sikkerhedsbrud erhvervsspionage[17]. Det kan derfor muligvis forklare, at kun 14 procent mener, de har haft et IT-sikkerhedsbrud – de har ganske enkelt ikke opdaget, at de har haft et brud, fordi bagmanden har skjult deres indtrængen.

Manglende IT-sikkerhed kan dog også give økonomiske konsekvenser på andre måder for virksomhederne. I maj 2018 træder den nye persondataforordning i kraft, og den kan udløse en bøde på op til 4 procent af en virksomheds omsætning eller EUR 20 millioner (den højeste værdi af de to), hvis virksomheden ikke lever op til de krav, der stilles i persondataforordningen. Hvis man som virksomhed er underlagt disse skærpede krav i persondataforordningen, kan man altså risikere en meget stor bøde, hvis man ved en revision fra myndighedernes side ikke lever op til kravene indeholdt i persondataforordningen.

6.2 De store potentielle konsekvenser medfører et behov for risikostyring

Ligesom andre risici, der indgår i en virksomheds risikostyring, bør virksomhederne også tage stilling til IT-sikkerhedsrisici. Det betyder, at virksomhederne skal overveje sandsynligheden for og påvirkningen fra et IT-sikkerhedsangreb samt arbejde med at mitigere denne risiko og have handlingsplaner for håndtering af et IT-sikkerhedsbrud, hvis de skulle komme ud for dette.

Under alle omstændigheder står det klart, at en virksomhed uden en tilstrækkelig IT-sikkerhed er mere sårbar overfor et IT sikkerhedsangreb og dermed i større risiko for et IT-sikkerhedsbrud, som kan få betydelige konsekvenser for virksomheden.

6.3 Få virksomheder bruger på nuværende tidspunkt IT-sikkerhed som en konkurrenceparameter, men antallet forventes at stige i fremtiden

Det er også blevet fremhævet, at IT-sikkerhed kan være en vigtig parameter i konkurrencedygtigheden på tværs af danske virksomheder, og IT-sikkerhed bør derfor være på agendaen for at styrke Danmarks position.[18] For at IT-

[15] Cisco, Annual Cybersecurity Rapport, 2017.

[16] Cisco, Annual Cybersecurity Rapport, 2017.

[17] Verizon, Data Breach Investigations Report, 2017.

[18] http://di.dk/dibusiness/nyheder/Pages/Goer-it-sikkerhed-til-en-konkurrenceparameter.aspx

sikkerhed kan blive en konkurrenceparameter kræver det dog, at man starter i den enkelte virksomhed, men det ses generelt ikke, at det er tilfældet udover ved virksomheder, der arbejder specifikt med IT-sikkerhedsløsninger.

Flere eksperter[19] peger på, at IT-sikkerhed for et par år tilbage var IT-chefens domæne. Dette har de seneste år – og særligt indenfor det seneste år – ændret sig således, at både finansdirektøren, direktionen og endda bestyrelsen har fået IT-sikkerhed på radaren. Det indikerer, at ledelsen generelt har fået mere viden om IT-sikkerhed. Derudover er årsagerne hertil ifølge eksperterne tredelt: frygt for IT-sikkerhedsbrud, lovgivningsmæssig krav samt muligheden for at bruge IT som en konkurrenceparameter. Først og fremmest er nogle virksomheder blevet mere opmærksomme på IT-sikkerhed på grund af de økonomisk konsekvenser ved ikke at have en tilstrækkelig IT-sikkerhed. De økonomiske konsekvenser bunder i frygt, som virksomhederne har fra medierne eller historier i deres professionelle eller private netværk. Derudover spiller regulering en rolle i forhold til de økonomiske konsekvenser, specielt den kommende persondataforordning. De direkte økonomiske konsekvenser driver dermed mange danske virksomheder til at øge deres IT-sikkerhedsniveau. Eksperterne forventer også, at persondataforordningen betyder, at flere virksomheder vil stille krav til deres leverandørers IT-sikkerhed for at sikre IT-sikkerheden gennem hele værdikæden. Flere eksperter peger ligeledes på, at man ser en tendens til, at virksomhederne i stigende grad benytter IT-sikkerhed som konkurrenceparameter, specielt hvis virksomheden har kommercielle interesser i andre lande. Indeværende undersøgelse viser dog, at kun 15 procent har implementeret IT-sikkerhedsforanstaltninger af kommercielle årsager, heraf 13 procent af indenlandske kommercielle årsager og 2 procent af udenlandske kommercielle årsager. I caseinterviewene blev IT-sikkerhed som konkurrenceparameter heller ikke set som en drivkraft for virksomhedernes IT-sikkerhedsarbejde.

Det er ikke lykkedes Monitor Deloitte at finde undersøgelser, der underbygger, at IT-sikkerhed bruges som en konkurrenceparameter udover i specifikke brancher med særlig regulering eller i virksomheder, der udbyder IT-løsninger. Dette tyder derfor på, at danske virksomheder stadigvæk oplever en begrænset kommerciel mulighed i øget IT-sikkerhed. Afsluttende ser alle eksperterne, at IT-sikkerhed i fremtiden vil blive en vigtig parameter i valget af samarbejdspartnere, ligesom man har set det med CSR[20], og at man i stigende grad ser, at kunder – både virksomheder og private forbrugere – stiller krav til IT-sikkerhed. Der er også flere af respondenterne i caseinterviewene, der forventer, at deres kunder vil stille øgede krav til IT-sikkerhed i fremtiden.

6.4 Myndighederne kan spille en central rolle i at løfte IT-sikkerheden i danske SMV'er

Hvis IT-sikkerhed i højere grad skal bruges som en konkurrenceparameter på tværs af danske virksomheder, som eksperterne ser muligheder i, kræver det, at der gøres en indsats på tværs af de danske virksomheder. Her kan myndighederne spille en central rolle. Som det blev vist i kapitel 5, er lovgivningen en drivkraft for, at virksomheder implementerer IT-sikkerhed, og 23 procent af danske SMV'er angiver også lovgivning eller regulering som primær årsag til, at man har arbejdet med IT-sikkerhed. Herunder har den kommende persondataforordning haft betydning for nogle af (case)virksomhedernes arbejde med IT-sikkerhed, og enkelte af casevirksomhederne beskriver også, hvordan persondataforordningen har haft betydning for deres arbejde med IT-sikkerhed.

Spørger man virksomhederne, om de synes, at man fra det offentliges side bør gøre mere på dette område, ønsker virksomhederne dog i høj grad selv at varetage IT-sikkerhed uden for meget indblanding fra myndighedernes side. Til gengæld er der fem af virksomhederne fra caseinterviewene, der foreslår, at man fra det offentliges side kunne udstede guidelines og vejledninger, der kan hjælpe virksomhederne til at navigere i IT-sikkerhed. Dette bekræftes af eksperter, der mener, at myndighederne bør lede indsatsen indenfor IT-sikkerhed og sætte et godt eksempel.

Bedre vejledning fra myndigheder kan potentielt gøre SMV'erne i stand til at håndtere IT-sikkerhed på et tilstrækkelig højt niveau og samtidig give dem kompetencerne til at stille krav til IT-sikkerheden hos deres leverandører, så IT-sikkerheden sikres i hele værdikæden. Her foreslår casevirksomhederne konkrete anbefalinger til, hvordan virksomheder skal arbejde med IT-sikkerhed, og eventuelt hvor man skal starte, hvis man ikke har arbejdet med IT-sikkerhed før. Derudover ville det også være fordelagtigt, hvis man fra det offentliges side kunne være en central instans for at dele information. Både casevirksomhederne og eksperter peger ligeledes på, at vejledning fra myndighedernes side kan være effektiv, men eksperterne lægger vægt på, at vejledningen bør være praktisk og implementerbar, så den er nem for virksomhederne at anvende. Samtidig peger eksperter dog på, at myndighe-

[19] Eksperter refererer til de udvalgte specialister, som Monitor Deloitte har interviewet i forbindelse med denne analyse.

[20] Corporate Social Responsibility: begreb, der ofte defineres, virksomhedernes samfundsansvar og ansvarlig ageren for eksempel ved at tage hensyn til menneskerettigheder, sociale vilkår, arbejdsforhold mv.

derne ikke må komme i en position, hvor de kan have en konkurrencevridende effekt ved for eksempel at tilgodese og vejlede udvalgte virksomheder fremfor andre.

6.5 Afrunding

Danmark har en høj grad af digitalisering og anvendelse af IT, hvilket skaber muligheder for vækst og innovation. Det øger dog også risikoen for IT-sikkerhedsangreb og dermed IT-sikkerhedsbrud, da IT-sikkerheden i Danmark ikke er fulgt med digitaliseringsgraden. Denne undersøgelse understreger dette billede og viser, at 39 procent af danske SMV'er ikke har et tilstrækkeligt IT-sikkerhedsniveau og dermed er sårbare overfor IT-sikkerhedsangreb. Det ses i særlig grad, at virksomhederne mangler essentielle IT-sikkerhedsforanstaltninger, idet næsten en fjerdedel ikke har implementeret disse foranstaltninger. Derudover er virksomhedernes indsats mod medarbejderne i forhold til IT-sikkerhed formaliseret i lav grad, og der er primært fokus på den mundtlige kommunikation fremfor formaliserede tiltag som træning af medarbejderne og dokumenteret IT-sikkerhedspolitik.

I SMV'ernes arbejde med IT-sikkerhed er særligt medarbejdernes handlinger og manglende viden om IT-sikkerhed en barriere, og det kræver en kulturændring i virksomhederne at overkomme denne barriere. Virksomhederne skaber denne kulturændring ved at holde fokus på kommunikation og øge medarbejdernes viden om IT-sikkerhed og -sikkerhedstrusler. Viden om IT-sikkerhed er generelt en vigtig faktor for IT-sikkerhed, og de IT-ansvarliges viden om IT-sikkerhed er en drivkraft for virksomhedernes IT-sikkerhed, idet det gør virksomhederne i stand til at identificere, hvilke trusler der er, og dermed, hvilke tiltag de er nødt til at implementere for at beskytte sig mod disse IT-sikkerhedstrusler.

Det er meget få virksomheder, der bruger IT-sikkerhed som en konkurrenceparameter, men eksperter peger på, at dette tal er steget de senere år, og de forventer også, at der vil ske en stigning fremadrettet. Hvis IT-sikkerhed skal blive en konkurrenceparameter, kræver det dog, at SMV'erne generelt får mere viden omkring risiciene ved manglende IT-sikkerhed. Denne viden vil ikke kun medføre, at virksomhederne selv vil øge deres IT-sikkerhedsniveau – de vil også være i stand til i højere grad at efterspørge et øget IT-sikkerhedsniveau hos leverandører og samarbejdspartnere. IT-sikkerhed vil dermed også blive en faktor, som virksomhederne kan anvende kommercielt.

7 Appendiks

Appendiks oversigt

7.1 Uddybende metodeafsnit vedrørende spørgeskemaundersøgelsen

Metodeafsnit der uddyber metoden bag spørgeskemaundersøgelsen. Afsnittet indeholder en definition af populationen, udvælgelse af respondenter, vægtning af respondenter, fremgangsmåde for spørgeskemaundersøgelsen, overvejelser omkring spørgsmål, kvalitet og kontrol af svar, samt hvordan respondenterne slutteligt er inddelt i den anvendte typologi.

7.2 Spørgeskema

Det fulde spørgeskema, som blev anvendt ved telefonindsamlingen.

7.3 Metode for interviews

Metodeafsnit der uddyber metoden bag de kvalitative caseinterviews. Afsnittet indeholder spørgeguiden for interviewene, hvordan respondenter blev udvalgt, hvordan interviewene forløb, samt hvordan interviewene efterfølgende blev dokumenteret.

7.4 Caseinterviews

Individuelle Casebeskrivelser baseret på interviews med de enkelte SMV'er.

7.1 Uddybende metodeafsnit vedrørende spørgeskemaundersøgelse

Der er udført en telefonbaseret spørgeskemaundersøgelse for at kunne etablere generelle konklusioner om danske SMV'er på en objektiv, repræsentativ og statistisk sikker måde. Formatet gør det muligt at indsamle en stor del objektiv kvantitativ information om emnet. Spørgeskemaundersøgelser muliggør værdifuld databehandling, der kan statistisk kvantificeres.

Undersøgelsen blev udført gennem telefonbaserede interviews for at sikre, at undersøgelsen har en så høj datakvalitet som muligt. Denne indsamlingsform er vurderet til at give de bedste forudsætninger for at nå ud til så mange virksomheder som muligt samtidig med, at validiteten i data er blevet så høj som mulig. Følgende årsager driver en bedre datakvalitet i telefonbaserede interviews frem for fx web-baserede interviews:

- Højere svarprocent: Telefoninterviews giver som udgangspunkt en højere svarprocent end andre metoder.
- Løbende styring af kvoter: Respondenter til interviewet udvælges løbende, som spørgeskemaundersøgelsen gennemføres. Dermed styres dataindsamlingen bedre end ved fx webbaserede spørgeskemaundersøgelser, hvor man er afhængig af, at de rigtige virksomheder besvarer undersøgelsen. På den måde har det været muligt at sikre nok besvarelser med de rigtige typer virksomheder således, at sample ikke er skævt udvalgt i forhold til populationen.
- Sikre relevant svarperson: Telefonbaserede interviews sikrer, at den mest relevante person i virksomhederne besvarer spørgeskemaet. Herved forventes det, at den meste relevante information af den bedste kvalitet opnås. I spørgeskemaundersøgelsen har der været fokus på at få direkte kontakt med virksomhedernes IT-sikkerhedsansvarlige, IT-chef eller sekundært ejer eller økonomiansvarlig. Hvis den IT-sikkerhedsansvarlige ikke har været tilgængelig den pågældende dag, er der efterfølgende blevet aftalt et møde med personen.

7.1.1 Population

Populationen til denne undersøgelse er danske SMV'er, som defineres forskelligt lidt afhængigt af kilde:

- DST definerer en SMV som værende en virksomhed med færre end 250 ansatte.[21]
- Europa-Kommissionen definerer en SMV som værende en virksomhed med færre end 250 ansatte samt en omsætning på maksimalt €50m samt maksimalt €43m i balanceopgørelse.[22]

Populationen til denne undersøgelse tager udgangspunkt i den definition, som DST benytter sig af og dermed ikke med et omsætnings- og balancekrav. Dog med den modifikation, at der udelukkende blev set på virksomheder med 5-249 ansatte. Virksomheder under 5 ansatte blev udelukket, fordi disse mindre selskaber typisk er enkeltmandsvirksomheder, som har en lav grad af IT-anvendelse. Med udgangspunkt i disse kriterier blev den samlede population til spørgeskemaundersøgelsen 81.016 virksomheder, som det fremgår af Tabel 4.

[21] http://www.dst.dk/Site/Dst/Udgivelser/nyt/GetAnalyse.aspx?cid=27867

[22] http://ec.europa.eu/growth/smes/business-friendly-environment/sme-definition/

Tabel 4: Population. Kilde: Wilke for Monitor Deloitte

	5-9 ansatte	10-19 ansatte	20-49 ansatte	50-99 ansatte	100-249 ansatte	**Total**
A Landbrug, skovbrug og fiskeri	1.922	697	245	83	29	2.976
B Råstofindvinding	34	27	47	39	11	158
C Industri	1.926	1.676	1.570	831	582	6.585
D Energiforsyning	167	136	126	19	46	494
E Vandforsyning og renovation	179	73	117	140	258	767
F Bygge og anlæg	3.420	2.040	1.242	403	211	7.316
G Handel	7.178	4.629	3.997	1.908	1.828	19.540
H Transport	1.220	870	684	279	262	3.315
I Hoteller og restauranter	3.104	2.262	1.556	400	279	7.601
J Information og kommunikation	1.167	769	605	252	158	2.951
K Finansiering og forsikring	615	336	286	170	149	1.556
L Ejendomshandel og udlejning	1.483	894	826	514	730	4.447
M Videnservice	2.134	1.231	984	428	339	5.116
N Rejsebureauer, rengøring og anden operationel service	1.531	863	717	339	230	3.680
P Undervisning	345	443	936	331	603	2.658
Q Sundhed og socialvæsen	2.683	1.729	1.202	489	744	6.847
R Kultur og fritid	788	599	532	179	99	2.197
S Andre serviceydelser m.v.	1.271	666	416	260	134	2.747
X Uoplyst aktivitet	27	22	10	3	3	65
Total	31.194	19.962	16.098	7.067	6.695	81.016

Populationen, som ligger til grund for undersøgelsen, er udtrukket fra virksomhedsdatabasen NN Data, som er baseret på Det Centrale Virksomhedsregister (CVR) samt virksomhedernes egne regnskaber.

Der er på populationsudtrækket anvendt filtre for at sortere i populationen. Wilke har indsat filtre på følgende virksomhedsformer:

- Dødsboer (frasorteres)
- Offentlige virksomheder (frasorteres)
- Virksomheden optræder kun i population under hovedaktivitet (primær branche)
- Selskabet er i normal drift

7.1.2 Udvælgelse af respondenter

Sample blev udvalgt som et kvoteinterval for hhv. virksomhedsstørrelse og branche med udgangspunkt i populationen vist i afsnit 7.1.1. For at muliggøre sammenligning med DST VITA blev der en minimum kvote på 100 interviews inden for hver af de brancher, som er i VITA. Ved samplingen er der indledningsvist disproportioneret på branche og antal ansatte. Dette fremgår også af Tabel 5 nedenfor. Denne disproportionering er sket for at sikre tilstrækkelig repræsentation af besvarelser fra de antalsmæssigt meget store virksomheder og fra antalsmæssigt små brancher. Sample i spørgeskemaundersøgelsen fordeler sig som vist i Tabel 5:

Tabel 5. Kvoter for sample. Kilde: Wilke for Monitor Deloitte

	Tilstræbet					Opnået	Statistisk usikkerhed
Branche	5-9 ansatte	10-19 ansatte	20-49 ansatte	50-99 ansatte	100-249 ansatte		
A Landbrug, skovbrug og fiskeri	30-50					34	15,4
B Råstofindvinding	5-15					7	30,1
C Industri	Min. 100					141	9,7
D Energiforsyning	5-15					13	30,7
E Vandforsyning og renovation	5-15					10	30,8
F Bygge og anlæg	Min. 100					120	9,7
G Handel	Min. 100					123	9,8
H Transport	Min. 100					103	9,7
I Hoteller og restauranter	50-70					51	12,6
J Information og kommunikation	Min. 100					83	9,6
K Finansiering og forsikring	5-15					12	30,9
L Ejendomshandel og udlejning	50-70					45	12,6
M Videnservice	Min. 100					103	9,7
N Rejsebureauer, rengøring og anden operationel service	Min. 100					103	9,7
P Undervisning	20-40					44	9,6
Q Sundhed og socialvæsen	20-40					23	17,9
R Kultur og fritid	10-30					17	21,8
S Andre serviceydelser m.v.	10-30					22	21,8
Total	142	239	239	239	141	1.054	
Statistisk usikkerhed (%)	8,2	6,3	6,3	6,2	8,2	3,1	

1.054 interviews har givet anledning til, at flere konklusioner kan bekræftes med høj statistisk sikkerhed. Det er derfor muligt at give nøjagtige konklusioner om flere segmenter i undersøgelsen. Dette er tilfældet, når den statistiske usikkerhed er under 10 procent. I denne undersøgelse har det derfor været muligt at sige noget med statistisk sikkerhed om følgende, som det fremgår af Tabel 5:

- Den samlede population af SMV'er i Danmark.
- 7 udvalgte brancher (C: Industri, F: Bygge og Anlæg, G: Handel, H: Transport, J: Information og kommunikation, M: Vidensservice, N: Rejsebureauer, rengøring og anden operationel service, P: Undervisning).
- Virksomhedsstørrelser (ikke fordelt på brancher).

7.1.3 Vægtning

Stikprøven er vægtet på henholdsvis antal ansatte og branche for at sikre, at stikprøven er repræsentativ. Denne vægtning er valgt for at sikre, at nettostikprøven får den rigtige fordeling ift. populationen. Vægtningen er lavet ud fra størrelsesforholdet mellem population og stikprøven. I Tabel 6 herunder ses forskellen på nettostikprøvens uvægtede og vægtede fordelinger.

Tabel 6: Vægtning af stikprøve. Kilde: Wilke for Monitor Deloitte

Branche	**Uvægtet**	**Vægtet**	**Ideal fordeling**
Landbrug, jagt, skovbrug og fiskeri	3,2%	3,7%	3,7%
Råstofindvinding	0,7%	0,2%	0,2%
Fremstillingsvirksomhed	13,4%	8,0%	8,0%
El-, gas- og fjernvarmeforsyning	1,2%	0,6%	0,6%
Vandforsyning; kloakvæsen, affaldshåndtering og rensning af	0,9%	0,9%	0,9%
Bygge- og anlægsvirksomhed	11,4%	8,9%	8,9%
Engroshandel og detailhandel; reparation af motorkøretøjer o	11,7%	24,1%	24,1%
Transport og godshåndtering	9,8%	4,1%	4,1%
Overnatningsfaciliteter og restaurationsvirksomhed	4,8%	9,5%	9,5%
Information og kommunikation	7,9%	3,7%	3,7%
Pengeinstitut- og finansvirksomhed, forsikring	1,1%	1,8%	1,8%
Fast ejendom	4,3%	5,7%	5,7%
Liberale, videnskabelige og tekniske tjenesteydelser	9,8%	6,3%	6,3%
Administrative tjenesteydelser og hjælpetjenester	9,8%	4,5%	4,5%
Undervisning	4,2%	3,2%	3,2%
Sundhedsvæsen og sociale foranstaltninger	2,2%	8,6%	8,6%
Kultur, forlystelser og sport	1,6%	2,8%	2,8%
Andre serviceydelser	2,1%	3,4%	3,4%
Antal ansatte	**Uvægtet**	**Vægtet**	**Ideal fordeling**
5-9	16%	39%	39%
10-19	24%	25%	25%
20-49	24%	20%	20%
50-99	23%	9%	9%
100-249	14%	8%	8%

7.1.4 Fremgangsmåde

Dataindsamling i det telefonbaserede spørgeskema forløb gennem følgende syv trin:

1. Spørgeskemaet blev udarbejdet i samarbejde med Erhvervsstyrelsen i september 2017.
2. Skemaet blev kontrolleret mht. spørgsmålenes formuleringer, svaralternativer og visningsbetingelser ved manuel gennemgang af skemaet og ved kontrol af tilfældigt genererede testinterview.
3. Sample blev løbende tilpasset, til de ønskede kvoter blev udviklet.
4. Der blev gennemført pilottest på undersøgelsen 27. og 28. september 2017. Datatjek efter pilottesten gav grundlag til ændringer i skema.
5. Dataindsamling: Interviewerne ringede til virksomhederne og fik kontakt med den relevante person. Enten blev interviewet gennemført med det samme, eller alternativt blev der lavet en aftale om, hvornår opkald kunne foregå.
6. Der blev foretaget løbende overvågning af kvoter samt kvalitetssikring, således der løbende blev holdt øje med, at det rigtige antal interview med de rigtige typer virksomheder blev opnået for at sikre et repræsentativt sample.
7. Data blev kontrolleret i forhold til dubletter, svarmønstre på tværs af udvalgte variable, afvigelser i forhold til den gennemsnitlige interviewtid og kontrol af de verbatime besvarelser.

7.1.5 Overvejelser omkring udformning af spørgeskema

Til at gennemføre det telefonbaserede spørgeskema, blev der udarbejdet et spørgeskema indeholdende 24 spørgsmål. Spørgeskemaet blev inddelt i tre kategorier:

- Del 1: Generelle oplysninger om virksomheden, til gruppering af virksomhederne.
- Del 2: Virksomhedens eksisterende forhold til risikostyring, -håndtering og –vurdering.
- Del 3: Virksomhedens arbejde med at reducere IT-sikkerhedsrelaterede risici.

Da IT-sikkerhed er et sensitivt område, var det en overvejelse, om virksomhederne kunne være tilbageholdende med at dele information. Derfor blev det vurderet hensigtsmæssigt at gøre spørgeskemaet anonymt, samt at udtrykke dette eksplicit i telefoninterviewet. Der var en antagelse om, at når respondenterne vidste, at deres svar ikke kunne spores tilbage til dem, ville de svare ærligt og ikke tilbageholde information. Samtidig blev enkelte af de indledende spørgsmål formuleret som indirekte spørgsmål, så der blev spurgt ind til, om der var kendskab til IT-sikkerhedsbrud hos samarbejdspartnere, leverandører eller kunder fremfor hos virksomheden selv. Denne tilgang blev valgt for at undgå, at virksomhederne følte, at spørgsmålet var for sensitivt.

IT-sikkerhed er ligeledes et komplekst område, og det var forventet, at respondenterne havde meget varierende indsigt i emnet. Derfor blev spørgsmålene holdt i et neutralt sprog uden komplekse og tekniske formuleringer.

7.1.6 Kvalitet og kontrol

Statistikken for undersøgelsens gennemførelse er vist i Tabel 7.

Tabel 7: Fra sample til gennemførte interviews. Kilde: Wilke for Monitor Deloitte

Emne	Antal
Bruttosample	16.165
Ugyldigt telefonnummer	372
Bortfald ved screening	1.989
Kvote fuld	596
Nettosample	13.208
Ikke trufne	10.345
Nægtere	1.809
Gennemført	1.054

Virksomheder/personer, som siger, at virksomheden enten ikke er i en af de adspurgte brancher eller ikke har 5-249 ansatte, er frascreenet. "Kvote fuld" er virksomheder, som passer ind i undersøgelsen, men blev valgt fra, da den ønskede mængde af besvarelser var opnået i specifikke branche områder.

7.1.7 Inddeling af virksomheder i typologi

Hver respondent inddeles efter deres niveau for IT-sikkerhed samt deres risikoprofil i tre arketyper. IT-sikkerhedsniveauet dækker i den sammenhæng over tre elementer; fysisk adgangskontrol, IT-sikkerhedsforanstaltninger og IT-sikkerhed relateret til medarbejdere og ledelse. Har en virksomhed således et lavt IT-sikkerhedsniveau, vil virksomheden være mere sårbar i tilfælde af et IT-sikkerhedsangreb. En virksomheds risikoprofil, hvor alvorligt et IT-sikkerhedsbrud vil være for virksomheden, og hvor stor sandsynligheden er for, at virksomheden bliver ramt. Jo højere risikoprofil, desto mere kritisk vil et IT-sikkerhedsbrud være for virksomheden.

7.1.7.1 Risikoprofil

Hver virksomhed undersøges for deres afhængighed af systemer, deres grad af brug af følsomme personoplysninger samt forretningskritiske informationer. Der spørges således ikke ind til, i hvilket omfang virksomheden gemmer denne type data, kun om virksomheden behandler denne type data. Monitor Deloitte vurderer, at de fleste virksomheder, som behandler disse typer data også gemmer dem. Set i lyset af denne overvejelse samt behovet for at reducere omfanget af spørgeskemaet er der således ikke spurgt konkret ind til, om virksomheden gemmer denne type data. Ved forretningskritiske informationer undersøges desuden, hvor udsat virksomheden ville være ved et

datalæk – fx ved læk af patenter, kunders fortrolige informationer eller lignende. Afsluttende vurderes hver enkelt virksomhed ud fra deres branche.

Risikoprofilen baseres på de fire spørgsmål, som fremgår af Tabel 8:

Tabel 8: Spørgsmål til vurdering af risikoprofil. Kilde: Monitor Deloitte.

Spørgsmål	Score
Spørgsmål 7: I hvor høj grad er jeres virksomhed afhængige af jeres IT-systemer for jeres daglige drift?	0 ("slet ikke") – 4 ("i høj grad")
Spørgsmål 8: I hvor høj grad behandler jeres systemer persondata med særlig risiko dvs. følsomme persondata, CPR-numre mm.	0 ("slet ikke") – 4 ("i høj grad")
Spørgsmål 9: Behandler jeres systemer data, som er forretningskritiske og vil medføre væsentlige problemer hvis de bliver delt eller hacket (fx forretningshemmeligheder og kundedatabaser)?	0 ("nej") – 1 ("ja")
Spørgsmål 9i: I hvor høj grad ville et brud på jeres systemer og dermed læk af forretningskritiske data være kritisk for jer?	0 ("Meget lidt") – 4 ("Forretningsgrundlag ville ikke længere eksistere")

Udover ovenstående fire spørgsmål får hver virksomhed tildelt en branchescoring. Dvs. en scoring afhængig af den branche virksomheden opererer i. Årsagen til, at denne vurdering er medtaget, er, at graden af følsom data og afhængigheden af IT-systemer vil være forskellig afhængig af branche. Branchescoringen går fra 1-3, og er beskrevet i detaljer herunder:

- Scoren 1: Systemer anvendes i varierende grad i virksomheder i denne branche. Følsomme data anvendes generelt i begrænset omfang – ofte i forbindelse med HR-arbejdet internt i virksomheden.
- Scoren 2: Systemer er en central del af arbejdet for virksomheder i denne branche, men graden af følsom data er meget varierende og typisk ikke høj for både følsomme personoplysninger og forretningskritiske typer.
- Score 3: Virksomheder i denne branche har en meget høj afhængighed af såvel personspecifikt samt forretningskritisk data. Derudover er systemer typisk centrale for deres drift.

Baseret på ovenstående er de 18 brancher inddelt i scoren 1-3. Brancherne er inddelt ud fra Deloitte Cyber Risks indsigt og arbejde med disse brancher og scoret efter Deloitte Cyber Risks erfaringer med kunder inden for de enkelte branchekategorier. Resultatet er, som følger af Tabel 9 herunder.

Tabel 9: Branchescoring. Kilde: Ekspertvurdering af Deloitte Cyber Risk & Monitor Deloitte

Branche	Score
Administrative tjenesteydelser og hjælpetjenester	2
Andre serviceydelser	2
Bygge- og anlægsvirksomhed	1
El-, gas- og fjernvarmeforsyning	3
Engroshandel og detailhandel; reparation af motorkøretøjer	1
Fast ejendom	1
Fremstillingsvirksomhed	2
Information og kommunikation	2
Kultur, forlystelser og sport	1
Landbrug, jagt, skovbrug og fiskeri	1
Liberale, videnskabelige og tekniske tjenesteydelser	3
Overnatningsfaciliteter og restaurationsvirksomhed	2
Pengeinstitut- og finansvirksomhed, forsikring	3
Råstofindvinding	1
Sundhedsvæsen og sociale foranstaltninger	3
Transport og godshåndtering	2
Undervisning	2
Vandforsyning; kloakvæsen, affaldshåndtering og rensning af	3

En følsomhedsanalyse af betydningen af branchescoringen fremgår af afsnittet Følsomhedsanalyse under kapitel 7.1.7.3.

Baseret på de fire spørgsmål fra Tabel 8 samt branchescoring fra Tabel 9 får hver virksomhed tildelt et antal point fra 1-16. Antallet af point definerer virksomhedens risikoprofil, som der redegøres for i detaljer i det efterfølgende afsnit.

Grænseværdier for risikoprofil

Scoringen fra 1-16 point inddeler virksomhederne i lav, middel og høj risikoprofil. Grænseværdierne for disse inddelinger er udført ved at dele dette interval i tre lige store størrelser: Lav: 1 til og med 6, Middel: 6 til og med 11, Høj: 11 til og med 16. Der er forskellige årsager til, at dette interval er valgt:

- Intervallerne er pointmæssigt lige store
- Alle virksomheder i undersøgelsen har en afhængighed til systemer, hvis de også håndterer følsomme personoplysninger eller forretningskritisk data. Omvendt vil en virksomhed, som har en lav grad af afhængighed overfor følsomme personoplysninger også have en lav grad af afhængighed af systemer. Dette betyder, at:

- En virksomhed med minimum afhængighed af systemer og følsom data dermed vil være i lav risikoprofil og dermed score 6 point eller derunder, uafhængig af brancherisiko
- En virksomhed med en høj afhængighed til enten systemer *eller* de forskellige følsomme data vil ende med en middel risikoprofil og dermed score mellem 6 og 11 point, uafhængig af brancherisiko
- En virksomhed med en høj afhængighed til systemer *og* de forskellige følsomme data vil ende med en høj risikoprofil uafhængig af brancherisiko.

Grænseværdierne for risikoprofilen er dermed sigende for virksomhedens udsathed ved et IT-sikkerhedsnedbrud eller datalæk.

7.1.7.2 IT-sikkerhedsniveau

IT-sikkerhedsniveauet vurderes ud fra 22 spørgsmål inden for emnerne; fysisk adgangskontrol, IT-sikkerhedsforanstaltninger og IT-sikkerhed ift. medarbejdere og ledelse. Hvert spørgsmål vægtes ud fra en vurdering af spørgsmålets vigtighed i forhold til IT-sikkerheden hos virksomheden. Samlet set giver dette en emneopdelt vægtning med hhv. 9%, 46% og 46% mellem de tre emner. Hvert spørgsmål har udover en vægtning en point-score, som går fra 0-4 baseret på spørgsmålets svarmulighed. Score og vægt fremgår af Tabel 10 herunder.

Tabel 10: Score og vægt IT-sikkerhedsniveau. Kilde: Monitor Deloitte

#	Spørgsmål	Score	Vægt
	Fysisk adgangskontrol		
1	Spørgsmål 24O: Hvilke foranstaltninger har I påbegyndt: (Fysisk adgangsstyring til virksomhedens kontorer gennem personlig adgangsnøgle (fx i form af personlig adgangskort eller chip - fysiske nøgler dækker	0-1	1
2	Spørgsmål 24P: Hvilke foranstaltninger har I påbegyndt: (Fysisk adgangsstyring til kritisk information (f.eks. adgangsstyring til server-adgang vha. personlig kode/kort/nøgle)?)	0-1	1
	IT-sikkerhedsforanstaltninger		
3	Spørgsmål 24B: Hvilke foranstaltninger har I påbegyndt: (Løbende IT-risikovurderinger (f.eks. baseret på ISO27001)?)	0-1	1
4	Spørgsmål 24C: Hvilke foranstaltninger har I påbegyndt: (Løbende intern IT-sikkerhedsanalyser og/eller IT-revision af jeres IT-systemer og hjemmesider?)	0-1	1
5	Spørgsmål 24D: Hvilke foranstaltninger har I påbegyndt: (Løbende ekstern IT-sikkerhedsanalyser og/eller IT-revision af jeres IT-systemer og hjemmesider?)	0-1	1
6	Spørgsmål 24E: Hvilke foranstaltninger har I påbegyndt: (Løbende vurderinger og opfølgning af medarbejderadgange til informationer og systemer?)	0-1	1
7	Spørgsmål 24F: Hvilke foranstaltninger har I påbegyndt: (Løbende overvågning og logning af sikkerheden i IT-systemer?)	0-1	0,5
8	Spørgsmål 24G: Hvilke foranstaltninger har I påbegyndt: (Samarbejde med eksterne rådgivere/samarbejdspartner inden for IT-sikkerhed?)	0-1	0,5
9	Spørgsmål 24H: Hvilke foranstaltninger har I påbegyndt: (Dokumenteret	0-1	1

	overblik over kritiske informationer og systemer?)		
10	Spørgsmål 24I: Hvilke foranstaltninger har I påbegyndt: (Dokumenterede og gennemtestede back-up procedurer?)	0-1	1
11	Spørgsmål 24J: Hvilke foranstaltninger har I påbegyndt: (Dokumenteret beredskabsplan?)	0-1	0,5
12	Spørgsmål 24K: Hvilke foranstaltninger har I påbegyndt: (Databehandler-aftale for håndtering af personfølsomme information?)	0-1	0,5
13	Spørgsmål 24L: Hvilke foranstaltninger har I påbegyndt: (Fast procedure for håndtering af personfølsomme information i virksomheden?)	0-1	1
14	Spørgsmål 24M: Hvilke foranstaltninger har I påbegyndt: (Systematiske og løbende opdateringer af IT-systemer og PC programmer?)	0-1	1
15	Spørgsmål 24N: Hvilke foranstaltninger har I påbegyndt: (Forsikringspolice, der dækker tab/omkostninger som følge af IT-sikkerhedshændelser)	0-1	0,5
	IT-sikkerhed ift. medarbejdere og ledelse		
16	Spørgsmål 4: Uddanner eller træner I jeres medarbejdere i IT-sikkerhed?	0-1	2
17	Spørgsmål 10: I hvor høj grad har ledelsen i virksomheden taget stilling til, hvordan IT-sikkerhed og databeskyttelse skal håndteres?	0-4	1
18	Spørgsmål 12A: Hvordan sikrer I, at medarbejderne er bevidste om informationssikkerheden i virksomheden? (Vi kommunikerer informationssikkerhed mundtligt.)	0-1	2
19	Spørgsmål 12B: Hvordan sikrer I, at medarbejderne er bevidste om informationssikkerheden i virksomheden? (Vi har en dokumenteret IT-sikkerhedspolitik (fx pjece).)	0-1	1
20	Spørgsmål 12C: Hvordan sikrer I, at medarbejderne er bevidste om informationssikkerheden i virksomheden? (Vi kommunikerer løbende den dokumenterede IT-sikkerhedspolitik (fx ved ny ansættelser eller årlige seancer).)	0-1	0,5
21	Spørgsmål 12D: Hvordan sikrer I, at medarbejderne er bevidste om informationssikkerheden i virksomheden? (Vi måler kontinuerligt medarbejdernes bevidsthed omkring sikkerhedstrusler)	0-1	0,5
22	Spørgsmål 24A: Hvilke foranstaltninger har I påbegyndt: (Udpeget en medarbejder som IT-sikkerhedsansvarlig?)	0-1	0,5

Samlet set går scoren fra 0-23. Niveauet for vægtningen redegøres for under afsnittet Vægtning og grænseværdier for IT-sikkerhedsniveauet.

Diskvalificering og ekstrapointgivende spørgsmål

To spørgsmål er udvalgt til at 'diskvalificere' en virksomheds IT-sikkerhedsniveau således, at virksomheden automatisk defineres med lavt IT-sikkerhedsniveau, uanset hvilket IT-sikkerhedsniveau denne virksomhed måtte have.

Disse to spørgsmål er:

- Spørgsmål 24I: Hvilke foranstaltninger har I påbegyndt: (Dokumenterede og gennemtestede back-up procedurer?)
- Spørgsmål 24M: Hvilke foranstaltninger har I påbegyndt: (Systematiske og løbende opdateringer af IT-systemer og PC programmer?)

En diskvalificering finder dermed sted, hvis der svares "Nej" eller "Ved ikke" til en af de ovenstående spørgsmål. Disse to spørgsmål er udvalgt til at diskvalificere virksomhedens IT-sikkerhedsniveau, fordi de vurderes til at være essentielle for IT-sikkerheden i en virksomhed. En dokumenteret og gennemtestet backup-procedure muliggør, at en virksomhed, som rammes af et IT-sikkerhedsangreb, relativt hurtigt kan få sine systemer op at køre igen. Samtidig er systematiske og løbende opdateringer centrale for IT-sikkerheden, fordi producenterne af IT-systemer og programmer løbende patcher, dvs. reparerer fejl og mangler i deres software for at reducere muligheden for, at et IT-sikkerhedsangreb går gennem deres systemer og programmer. Således er dokumenteret og gennemtestet backup og systematiske og løbende opdateringer af IT-systemer de første tiltag, en virksomhed anbefales at udføre, såfremt disse ikke er på plads i virksomheden.

Ud over de diskvalificerende spørgsmål er to spørgsmål, spørgsmål 4 og 12A, udvalgt til at være ekstrapointgivende. Årsagen hertil er, at Monitor Deloitte, efter omfattende case-interviews med danske SMV'er, har konstateret, at mange virksomheders IT-sikkerhed går gennem deres medarbejdere og er en vigtig del af IT-sikkerheden i SMV'erne. Herunder er træning af enkelte eller flere medarbejdere samt uformel kommunikation de mest grundlæggende tiltag til at skabe opmærksomhed omkring IT-sikkerhed for sine medarbejdere. Dette underbygges endvidere af Deloitte Cyber Risk, som vurderer, at disse to tiltag er mere væsentlige end de andre tiltag, når der tales om medarbejdere. Af denne årsag er disse to spørgsmål tillagt mere værdi.

Vægtning og grænseværdier for IT-sikkerhedsniveauet

Grænseværdierne for inddelingen af virksomhederne i lavt, middel og højt IT-sikkerhedsniveau er baseret på en vurdering af, hvad der er grundlæggende for IT-sikkerheden i virksomheden. Alle spørgsmål, der vurderes nødvendige for at have en grundlæggende IT-sikkerhed, som beskrevet i kapitel 4, er vægtet med 1, og de giver tilsammen 14 point. Alle spørgsmål, der vurderes som avancerede tiltag, som beskrevet i kapitel 4, vægtes med 0,5. Vurderingen af spørgsmål for hhv. grundlæggende og avancerede tiltag er baseret på Deloittes Cyber Risks kendskab på området, DST VITA undersøgelsen samt Sikkerhedstjekket.dk. Summen af de grundlæggende spørgsmål, 14, er sat som den nedre grænse for, at virksomheden vurderes som havende en middel IT-sikkerhedsniveau. Man skal således have 14 point eller derover for at opnå et middel IT-sikkerhedsniveau. For at opnå et højt IT-sikkerhedsniveau skal man have minimum halvdelen af de avancerede samt de grundlæggende tiltag, hvilket svarer til, at man skal have minimum 18,5 point for at vurderes til at have en høj IT-sikkerhedsniveau. Grænsen på de 18,5 er valgt, fordi dette skiller intervallet i to lige store dele.

Svarer virksomheden "Ved ikke" på et spørgsmål, betragtes det på samme måde, som svaret "Nej" og giver således ikke point. Har virksomheden således ikke været i stand til at svare på spørgsmål, må dette være et udtryk for, at den interviewede person enten ikke har den specifikke viden, eller at virksomheden ikke har den specifikke foranstaltning. Begge tilfælde er ikke optimalt og bør således ikke give anledning til point på samme måde som et "Ja". Spørgsmålet er dernæst, om "Ved ikke" bør give strafpoint, dvs. en yderligere reduktion i point. Dette vurderes til at være for hårdt, da virksomheden principielt kunne have foranstaltningen.

Dermed ser grænseværdierne for IT-sikkerhedsniveauet således ud:

- 0-13,9: Lavt IT-sikkerhedsniveau
- 14-18,4: Middel IT-sikkerhedsniveau
- 18,5-23: Højt IT-sikkerhedsniveau

Det skal bemærkes, at der er tre spørgsmål, der er justeret ud fra, hvad man har svaret i andre spørgsmål. Har man i spørgsmål 8 svaret, at man slet ikke har følsom data, får man automatisk point i 24K om databehandleraftale for personfølsom data og i spørgsmål 24L om fast procedure for håndtering af personfølsom data, da det vurderes, at man ikke skal straffes for ikke at have implementeret disse ting, hvis man ikke har personfølsom data. Har man i spørgsmål 15 svaret, at man har outsourcet hele virksomhedens IT, får man automatisk point i spørgsmål

24P omkring adgangssikring til serveren, da det vurderes ud fra Deloitte Cyber Risks omfattende branchekendskab, at en outsourcing-partner som udgangspunkt vil have fysisk adgangskontrol til servere.

7.1.7.3 Resultater

En virksomheds risikoprofil og IT-sikkerhedsniveau placerer virksomheden i en arketype, hvor man enten har et lavt IT-sikkerhedsniveau ift. risikoprofil (3), tilstrækkeligt IT-sikkerhedsniveau ift. risikoprofil (2) eller højt IT-sikkerhedsniveau ift. risikoprofil (1). Ved at bruge de vægtninger, som er beskrevet i detaljer i appendiks 7.1.3, der er tilknyttet de forskellige respondenter, kan man med statistisk signifikans sige noget om populationens fordeling inden for disse arketyper.

Med denne tilgang fordeler virksomhederne i spørgeskemaundersøgelsen sig således:

Tabel 11: Uvægtet fordeling af respondenter. Kilde: Monitor Deloitte

	Højt IT-sikkerhedsniveau	Middel IT-sikkerhedsniveau	Lav IT-sikkerhedsniveau	Total
Høj risikoprofil	84	112	81	277
Middel risikoprofil	79	182	218	479
Lav risikoprofil	20	82	196	298
Total	**183**	**376**	**495**	**1.054**

Således har:

- 183 virksomheder et højt IT-sikkerhedsniveau
- 376 virksomheder har et middel IT-sikkerhedsniveau
- 495 virksomheder har et lavt IT-sikkerhedsniveau

Ovenstående skal naturligvis ses i lyset af virksomhedens objektive risikoprofil, fordi virksomhederne har forskellig grad af udsathed.

Samlet set er fordelingen inden for arketyperne, som det fremgår af nedenstående **Tabel 12**:

Tabel 12: Fordeling af arketyper til virksomhedstypologi. Kilde: Monitor Deloitte

	Arketype, antal	Arketype, vægtet	Andel i procent	Andel i procent, vægtet
1 (mere end tilstrækkelig)	181	153,4	17%	**15%**
2 (tilstrækkelig)	462	485,5	44%	**46%**
3 (utilstrækkelig)	411	415,1	39%	**39%**
Total	1.054	1054,0		

Konklusionen er altså, at:

- 15% af danske SMV'er har et IT-sikkerhedsniveau, som er mere end tilstrækkeligt
- 46% af danske SMV'er har et IT-sikkerhedsniveau, som er tilstrækkeligt
- 39% af danske SMV'er har et IT-sikkerhedsniveau, som ikke er tilstrækkeligt

Følsomhedsanalyse ved udelukning af branchescoring

Resultatet fra Tabel 11 kan sidestilles med tilsvarende resultater, men hvor branchescoringen er udeladt. Scoringsintervallet er lavet i tre lige store intervaller. Branchescoringen er som nævnt fra 1-3 point. Således vil pointskalaen samlet set blive reduceret med 3 enheder på maksimalscoren fra 16 til 13 og med 1 point i begyndelsesscoren fra 1 til 0. Det samlede interval ville således være 0-13.

Tabel 13: Uvægtet fordeling af respondenter uden branchescoring. Kilde: Monitor Deloitte

	Højt IT-sikkerhedsniveau	Middel IT-sikkerhedsniveau	Lav IT-sikkerhedsniveau	Total
Høj risiko	85	113	83	281
Middel risiko	82	173	222	477
Lav risiko	16	90	190	296
Total	**183**	**376**	**495**	**1054**

Resultatet af denne ændring i pointskalaen fremgår af Tabel 13 og viser, at ændringerne er minimale. Således rykkes ca. 4 virksomheder fra middel til høj risiko, og 2 virksomheder rykkes fra lav til middelrisiko. Denne ændring er dermed i omegnen af 1% af den samlede sample størrelse, og branchescoringen har derfor kun en begrænset effekt på de endelige resultater.

7.2 Spørgeskema

På vegne af Erhvervsstyrelsen gennemfører Wilke og Deloitte i øjeblikket en kortlægning, som skal vise status for IT-sikkerhed og ansvarlig datahåndtering i danske små og mellemstore virksomheder.

I den sammenhæng udfører vi en række interviews med danske virksomheder på tværs af brancher. Jeres virksomhed er blevet udvalgt til at deltage og vi søger i den sammenhæng den ansvarlige for IT-sikkerhed i jeres virksomhed til et kort telefoninterview på ca. 10 minutter.

Telefoninterviewet er anonymt og besvarelserne vil alene blive brugt i aggregeret form således, at ingen informationer kan spores til jeres besvarelser.

[*Hvis der ikke kan identificeres en IT-sikkerhedsansvarlig i virksomheden så er hierarkiet følgende: 1) IT-ansvarlig, 2) virksomhedens direktør, 3) økonomichef, 4) virksomhedens ejer*]

[*Evt. supplerende information hvis der er behov for at præsentere opgaven yderligere for respondenten:* Baggrunden for projektet er, at dansk erhvervsliv oplever flere og flere IT-sikkerhedshændelser. Disse IT-sikkerhedshændelser påvirker virksomhedernes systemer og rummer en risiko for, at personfølsomme- eller forretningskritiske data lækkes til skade for virksomheden, samarbejdspartnere og kunder. På baggrund heraf ønsker Erhvervsstyrelsen indsigt i, hvordan danske små og mellemstore virksomheder arbejder med IT-sikkerhed og datahåndtering i dag uafhængigt af, om jeres IT og IT-sikkerhed er udliciteret til underleverandører.]

Erhvervsstyrelsen og Wilke sætter pris på jeres bidrag. Gennem jeres besvarelser vil I have indflydelse på de politiske tiltag, som vil blive iværksat på området.

q1 - 1.

Indledningsvis vil vi gerne vide lidt mere om jeres virksomhed.

Hvilken branche tilhører jeres virksomhed?

(Læs ikke op)

❍ Landbrug, jagt, skovbrug og fiskeri
❍ Råstofindvinding
❍ Fremstillingsvirksomhed
❍ El-, gas- og fjernvarmeforsyning
❍ Vandforsyning; kloakvæsen, affaldshåndtering og rensning af jord og grundvand
❍ Bygge- og anlægsvirksomhed
❍ Engroshandel og detailhandel; reparation af motorkøretøjer og motorcykler
❍ Transport og godshåndtering
❍ Overnatningsfaciliteter og restaurationsvirksomhed
❍ Information og kommunikation
❍ Pengeinstitut- og finansvirksomhed, forsikring
❍ Fast ejendom
❍ Liberale, videnskabelige og tekniske tjenesteydelser
❍ Administrative tjenesteydelser og hjælpetjenester
❍ Offentlig forvaltning og forsvar; socialsikring→ Frascreenes
❍ Undervisning
❍ Sundhedsvæsen og sociale foranstaltninger
❍ Kultur, forlystelser og sport
❍ Andre serviceydelser
❍ Virksomheden er lukket → Frascreenes

q2 - 2.

Hvor mange medarbejdere er direkte ansat i jeres virksomhed?

(Læs ikke op)

❍ 0-4 → Frascreenes
❍ 5-9
❍ 10-19
❍ 20-49
❍ 50-99
❍ 100-249
❍ 250 eller derover → Frascreenes

q3 - 3.

Hvilken primær rolle har du i virksomheden?

(Læs ikke op)

❍ It-sikkerhedsansvarlig
❍ It-ansvarlig
❍ Virksomhedens direktør
❍ Virksomhedens ejer
❍ Økonomichef
❍ Andet

q4 - 4.

Uddanner eller træner I jeres medarbejdere i IT-sikkerhed?

(Læs ikke op)

❍ Nej
❍ Ja, enkelte medarbejdere
❍ Ja, alle medarbejdere
❍ Ved ikke

q5 - 5.

Har du kendskab til, om nogle af jeres samarbejdspartnere har været udsat for et IT-sikkerhedsbrud, dvs. datalæk eller systemnedbrud som følge af hackerangreb?

(Læs ikke op)

❍ Nej
❍ Ja
❍ Ja, flere

q7 - 7.

I hvor høj grad er jeres virksomhed afhængig af jeres IT-systemer for jeres daglige drift?

(Læs op)

❍ 1 slet ikke
❍ 2
❍ 3
❍ 4
❍ 5 I høj grad
❍ Ved ikke

q8 - 8.

I hvor høj grad gemmer jeres systemer persondata med særlig risiko dvs. følsomme persondata, CPR-numre mm..

1 slet ikke

❍ 1 slet ikke
❍ 2
❍ 3
❍ 4
❍ 5 I høj grad
❍ Ved ikke

q9 - 9.

Gemmer jeres systemer data, som er forretningskritiske og vil medføre væsentlige problemer, hvis de bliver delt eller hacket (fx forretningshemmeligheder og kundedatabaser)?

(Læs ikke op)

❍ Ja
❍ Nej
❍ Ved ikke

Q9-9i. (hvis svaret er ja i q9)

I hvor høj grad ville et brud på jeres systemer og dermed læk af forretningskritiske data være kritisk for jer?

(Læs op)

❍ 1 Det ville påvirke vores forretningsgrundlag meget lidt
❍ 2
❍ 3
❍ 4
❍ 5 Vores forretningsgrundlag ville ikke længere eksistere, og vi ville lukke forretningen
❍ Ved ikke

i100

Vi vil nu gerne undersøge nærmere, hvordan jeres virksomhed arbejder med at forhindre sikkerhedsbrud relaterede til jeres IT-systemer.

q10 - 10.

I hvor høj grad har ledelsen i virksomheden taget stilling til, hvordan IT-sikkerhed og databeskyttelse skal håndteres?

(Læs op)

❍ 1 slet ikke
❍ 2
❍ 3
❍ 4
❍ 5 I høj grad

q11 - 11.

Hvad ser I som de væsentligste IT-relaterede sikkerhedstrusler for jeres virksomhed?

(Læs ikke op)

○ Phishing angreb (Mail hvor afsender udgivers sig for en anden med henblik på at kompromittere IT-sikkerheden)
○ Ransomware (Skadelige programmer, som installeres og låser computeren)
○ Hacket hjemmeside og/eller IT-system
○ Tab og/eller tyveri af medier (USB, CD, bærbare PC, servers, mv.) med fortrolig information
○ Sabotage/tyveri udført af tidligere medarbejder
○ Direktørsvindel (Hackere som udgiver sig for at være direktøren og forsøger at få overført penge til udenlandske konti)
○ Social Engineering (hackerangreb ved fysisk eller telefonisk henvendelse)
○ DDoS/DoS-angreb (hackerangreb hvor systemer/hjemmesider eksponeret på internettet, bliver bombarderet med falske og ondsindet forespørgsler/besøg, med henblik på at gøre systemet/hjemmesiden utilgængelig
○ Andet

q12 - 12.

Hvordan sikrer I, at medarbejderne er bevidste om informationssikkerheden i virksomheden?

(Læs op)

	Ja	Nej	Ved ikke (Læs ikke op)
Vi kommunikerer informationssikkerhed mundtligt.			
Vi har en dokumenteret IT-sikkerhedspolitik (fx pjece).	☐	☐	☐
Vi kommunikerer løbende den dokumenterede IT-sikkerhedspolitik (fx ved nyansættelser eller årlige seancer).	☐	☐	☐
Vi måler kontinuerligt medarbejdernes bevidsthed omkring sikkerhedstrusler	☐	☐	☐

q15 - 15.

Har jeres virksomhed udliciteret dele eller hele af IT samt håndtering af IT-sikkerhed?

(Læs ikke op)

❍ Nej
❍ Ja, dele af vores IT
❍ Ja, hele vores IT

q16 - 16.
Har jeres virksomhed haft et brud på IT-sikkerheden, som har påvirket den normale drift?

(Med brud på sikkerheden menes, at virksomhedens IT-systemer eller data skades eller gøres utilgængelige. Data kan fx være kundeoplysninger, regnskabsdata mv)

(Læs op)

❍ Ja, indenfor de seneste 12 måneder
❍ Ja, for mere end 12 måneder siden
❍ Dette kan ikke siges med sikkerhed
❍ Nej
❍ Ved ikke (Læs ikke op)

q17i - q17.i

Hvor mange sikkerhedsbrud har I haft de sidste 12 måneder?

(Læs ikke op)

❍ 1-5
❍ 6-10
❍ Over 10
❍ Ved ikke

q17ii - 17.ii

Hvilken type sikkerhedsbrud oplevede i?

(Læs ikke op)

○ Phishing angreb (Mail hvor afsender udgivers sig for en anden med henblik på at kompromittere IT-sikkerheden)
○ Ransomware (Skadelige programmer, som installeres og låser computeren)
○ Direktørsvindel
○ Hacket hjemmeside og/eller IT-system
○ Social Engineering (hackerangreb ved fysisk eller telefonisk henvendelse)
○ Tab og/eller tyveri af medier (USB, CD, bærbare PC, servers, mv.) med fortrolig information
○ Sabotage/tyveri udført af tidligere medarbejder
○ Andet, noter:_____

q17iii - 17.iii

Hvordan blev sikkerhedsbruddet identificeret?

(Læs ikke op)

○ Ved henvendelse fra intern medarbejder
○ Ved henvendelse fra samarbejdspartner
○ Ved henvendelse fra kunde
○ Ved notifikation fra overvågning og logningssystem
○ Ved brud på systemtilgængelighed
○ Som følge af IT-revision og/eller IT-sikkerhedsanalyser
○ Ved en tilfældighed
○ Andet

q18 - 18.

Hvad har de samlede økonomiske omkostninger ved sikkerhedsbruddet været?

❍ Angiv ca. beløb:_____
❍ Ved ikke (Læs ikke op)

q19 - 19.

Hvilke type omkostninger har I haft i forbindelse med sikkerhedsbruddet?

(Læs ikke op)

○ Omkostning til ekstern rådgivning og assistance ved sikkerhedsbrud
○ Tab ved betaling af falske faktura eller betalingsoverførelser (f.eks. ved direktørsvindel)
○ Betaling af løsesum ved ransomware angreb
○ Tab af produktion og/eller data ved brud på systemtilgængelighed (f.eks. utilgængelighed i mail- og fælles-drev-system)
○ Tab af image ved offentlig kendt sikkerhedsbrud
○ Tabte forretningsmuligheder
○ Andet

q22 - 22.

Er der tale om faktorer, som har haft direkte konsekvenser for jeres virksomhed?

❍ Ja
❍ Nej

(Hvis ja, gå til 22a, ellers i122)

Q22a Hvilke konsekvenser har det haft? (interviewer noterer svar i de(n) korrekte kategori)

(Læs op)

Forringelse af virksomhedens image/rygte
Tab af ordrer/markedsandele
Har opgivet eller udskudt investeringer fx i digitalisering eller ny teknologi
Andre konsekvenser

i122

De følgende spørgsmål går i detaljer med, hvordan jeres virksomhed arbejder forebyggende med at reducere sin risiko på området.

q24 - 24.

Hvilke foranstaltninger har I påbegyndt:

(Læs op)

	Ja	Nej	Ved ikke (Læs ikke op)
	☐	☐	☐
Løbende IT-risikovurderinger (f.eks. baseret på ISO27001)?	☐	☐	☐
Løbende intern IT-sikkerhedsanalyser og/eller IT-revision af jeres IT-systemer og hjemmesider?	☐	☐	☐
Løbende intern IT-sikkerhedsanalyser og/eller IT-revision af jeres IT-systemer og hjemmesider?	☐	☐	☐
Løbende vurderinger og opfølgning af medarbejderadgange til informationer og systemer?	☐	☐	☐
Løbende overvågning og logning af sikkerheden i IT-systemer?	☐	☐	☐
Samarbejde med eksterne rådgivere/samarbejdspartner inden for IT-sikkerhed?	☐	☐	☐
Dokumenteret overblik over kritiske informationer og systemer?	☐	☐	☐
Dokumenterede og gennemtestede back-up procedurer?	☐	☐	☐
Dokumenteret beredskabsplan?	☐	☐	☐

	Ja	Nej	Ved ikke (Læs ikke op)
Databehandleraftale for håndtering af personfølsomme information?	☐	☐	☐
Fast procedure for håndtering af personfølsomme information i virksomheden?	☐	☐	☐
Systematiske og løbende opdateringer af IT-systemer og PC programmer?	☐	☐	☐
Forsikringspolice, der dækker tab/omkostninger som følge af IT-sikkerhedshændelser	☐	☐	☐
Fysisk adgangsstyring til virksomhedens kontorer gennem personlig adgangsnøgle (fx i form af personlig adgangskort eller chip - fysiske nøgler dækker ikke over dette)?	☐	☐	☐
Fysisk adgangsstyring til kritisk information (f.eks. adgangsstyring til server-adgang vha. personlig kode/kort/nøgle)?	☐	☐	☐

q26 - 26. (single)

Hvad har været den primære årsag til, at jeres virksomhed har iværksat de nævnte IT-sikkerhedsforanstaltninger?

(Læs op)

- ○ Brud på IT-sikkerheden
- ○ Lovgivnings- eller reguleringsmæssige årsager
- ○ Indenlandske kommercielle årsager, fx krav fra samarbejdspartnere, kunder osv.
- ○ Udenlandske kommercielle årsager, fx krav fra samarbejdspartnere, kunder osv.
- ○ Andre årsager
- ○ Ved ikke (læs ikke op)

q28 - 28.

Må vi kontakte dig igen, hvis vi har uddybende spørgsmål?

(Læs ikke op)

- ❍ Ja
- ❍ Nej

Dette var afslutning på spørgeskemaet.

Erhvervsstyrelsen, Deloitte og Wilke vil gerne takke dig for at deltage i denne undersøgelse. Dit input vil være afgørende for Erhvervsstyrelsens videre arbejde på dette område til gavn for danske virksomheder og landet som helhed.

Tak for hjælpen.

7.3 Metode for interviews

7.3.1 Interviewguide

Til at udføre caseinterviewene blev der på forhånd udarbejdet en interviewguide, som skulle fungere som styrepind for intervieweren og sikre, at alle relevante områder blev afdækket. Da der er tale om en guide, var det muligt for intervieweren at afvige fra denne og stille opfølgende og uddybende spørgsmål i det omfang, det var relevant. Indledningsvist var der spørgsmål om virksomheden for at forstå virksomheden, dens situation og konteksten bedre. Dette blev efterfulgt af spørgsmål specifikt rettet mod virksomhedens håndtering af IT-sikkerhed. Næste afsnit omhandlede drivere og barrierer for at øge virksomhedens IT-sikkerhed, og fokus var på i høj grad at forstå, hvad der ligger til grund for virksomheders beslutninger omkring IT-sikkerhed. Herunder også hvilke konsekvenser (positive og negative), som virksomheden har oplevet ved at øge/ikke øge IT-sikkerheden. Sidste afsnit i spørgeguiden omhandler virksomhedens forventninger til IT-sikkerhed i fremtiden.

Spørgsmålene i interviewguiden var åbne, og der var ved mange spørgsmål givet eksempler på uddybende/opfølgende spørgsmål. Formuleringen og rækkefølgen af spørgsmålene i de enkelte interviews afhang dog af respondenten, respondentens svar og interviewets forløb.

7.3.1.1 Spørgeguide til case-interviews

Interviewguide til interview om IT-sikkerhed og forsvarlig datahåndtering i danske SMV'er

Deloitte gennemfører i øjeblikket en analyse for Erhvervsstyrelsen, som skal vise status for IT-sikkerhed og forsvarlig datahåndtering i danske små og mellemstore virksomheder.

Baggrunden for denne undersøgelse er, at der sker flere sikkerhedsbrud i Danmark, hvilket kan have store konsekvenser for de berørte virksomheder. I takt med at virksomheder håndterer og lagrer mere data, øges konsekvenserne ved et sikkerhedsbrud, og vi ser samtidig flere og flere sikkerhedsbrud i Danmark, f.eks. i sommer hos Mærsk, som medførte store omkostninger for virksomheden.

I den sammenhæng udfører vi en række interviews med danske virksomheder på tværs af brancher med henblik på at afdække niveauet samt drivere og barrierer for at øge IT-sikkerhed.

Vi vil derfor gerne forstå jeres virksomheds arbejde med IT-sikkerhed. Hvis du har nogle interessante pointer og input, vil vi gerne bruge din virksomhed som case.

Erhvervsstyrelsen og Deloitte sætter pris på jeres bidrag. Gennem jeres besvarelser vil I have indflydelse på de politiske tiltag, som vil blive iværksat på området.

Vi vil i dette interview først komme ind på nogle indledende spørgsmål omkring jeres virksomhed for at forstå denne bedre. Dernæst vil vi gerne høre mere om jeres arbejde med IT-sikkerhed efterfulgt af de drivere og barrierer, I ser for at øge jeres IT-sikkerhed. Til sidst vil vi gerne høre mere om, hvordan I forventer at arbejde med IT-sikkerhed fremadrettet.

A. Indledende spørgsmål om virksomheden

Som det første vil vi gerne vide lidt mere om jeres virksomhed og IT-håndtering i jeres virksomhed.

- Hvilken primær rolle har du i virksomheden? / Kan du fortælle om din rolle i virksomheden?
- Hvilken type kunder har I (her tænkes B2B, B2C, B2G samt brancher og størrelser)?
- I hvilken grad orienterer jeres forretning sig mod internationale markeder?
- Hvor i værdikæden ligger jeres virksomhed?
- Hvilken type data håndterer I i jeres virksomhed? (Alternativt: Håndterer I personfølsomme eller andre særligt følsomme data?)

   a. Personfølsomme data (fx. CPR-numre, sundhedsoplysninger eller andre personfølsomme informationer)
   b. Forretningskritisk information (fx forretningshemmelige, kundedatabase og andre forretningskritiske data)
   c. Hvor kritisk ville et IT-sikkerhedsbrud, hvor forretningskritiske data blev lækket, være for jeres virksomhed (her er det vigtigt at undersøge det samlede *impact* af et evt. læk)?
- Har I systemer, der er kritiske for jeres forretning?
   a. Hvordan vil det påvirke jeres forretning, hvis disse systemer kompromitteres/hackes?
- Har I outsourcet hele eller dele af jeres IT?
   a. Hvad betyder det for jeres IT-sikkerhed, at I har valgt at udlicitere jeres IT?
   b. Hvilken udbyder bruger I?
      i. Må vi få kontaktoplysningerne på jeres leverandør? Vi vil ikke spørge ind til jeres specifikke forhold, men vi vil gerne forstå hele værdikæden, hvorfor det er interessant at tale med to i samme værdikæde.
- Har I en forsikring, der dækker IT-sikkerhedsbrud?
- Hvordan sikrer I fysisk adgang til jeres servere, data og kontor? (Fysisk sikkerhed)

   a. Spørg ind til fysisk adgangsstyring til kritisk information (f.eks. adgangsstyring til server-adgang vha. personlig kode/kort/nøgle) og fysisk adgangsstyring til jeres virksomheds kontorer gennem personlig adgangsnøgle (fx i form af personlig adgangskort eller chip - fysiske nøgler dækker ikke over dette)?

B. Virksomhedens nuværende indsats ift. IT-sikkerhed og forsvarlig datahåndtering

Som det næste vil vi gerne vide lidt mere om, hvordan jeres virksomhed arbejder med at forhindre sikkerhedsbrud relaterede til jeres IT-systemer.

- Hvordan arbejder I med IT-sikkerhed i jeres virksomhed?
- Hvordan er jeres evne til at vurdere og håndtere IT-sikkerhedsrelaterede risici?
- Hvordan får I information om IT-sikkerhed, IT-sikkerhedstrusler og produkter på markedet?
- Hvordan sikrer I, at jeres medarbejdere har tilstrækkelig viden om og evner til at sikre IT-sikkerheden? (Medarbejderrelateret sikkerhed)
   a. Spørg ind til uddannelse og træning af medarbejdere, om ledelsen har taget stilling IT-sikkerhed, hvordan det sikres, at medarbejderne er bevidste om informationssikkerheden, om der er en IT-sikkerhedsansvarlig, og om de har en sikkerhedscertificering
- Har I foretaget investeringer i jeres IT-sikkerhed?
   a. Hvilke investeringer har I foretaget? (Teknisk IT-sikkerhed)
   b. Spørg ind til løbende IT-risikovurderinger (f.eks. baseret på ISO27001), løbende IT-sikkerhedsanalyser og/eller IT-revision af jeres IT-systemer og hjemmesider, løbende overvågning og logning af sikkerheden i IT-systemer, om de har et dokumenteret overblik over kritiske informationer og systemer, dokumenterede og gennemtestede backup-procedurer, en dokumenteret beredskabsplan, en databehandleraftale for håndtering af personfølsomme information, en fast proce-

dure for håndtering af personfølsomme information i virksomheden, og om de laver systematiske og løbende opdateringer af IT-systemer og PC programmer)

- Hvad var baggrunden for jeres investeringer? (husk uddybende forklaring) (støtteskema)
    a. Brud på IT-sikkerheden
    b. Lovgivnings- eller reguleringsmæssige årsager
    c. Indenlandske kommercielle årsager, fx krav fra samarbejdspartnere, kunder osv. eller andre forretningsmæssige forhold relateret til aktiviteter i Danmark
    d. Udenlandske kommercielle årsager, fx krav fra samarbejdspartnere, kunder osv., eller andre forretningsmæssige forhold relateret til internationale aktiviteter
- Har I tidligere oplevet, at jeres IT-sikkerhedsniveau ikke var tilstrækkelig og fik konsekvenser for jeres forretning?
    a. Hvilke konsekvenser oplevede I?

C. Drivere og barrierer for at øge IT-sikkerheden

De følgende spørgsmål går i dybden med, hvordan I har arbejdet med jeres IT-sikkerhed og hvilke overvejelser, I har gjort jer omkring dette, herunder hvilke drivere og barriere, I har oplevet i jeres arbejde med IT-sikkerhed

- Hvilke overvejelser lå bag beslutningen om at implementere nye tiltag?
- Hvilke barrierer oplevede I ved beslutningen om og implementeringen af disse tiltag, og hvordan overvandt I disse?
    a. Hvorfor anså I det for værende nødvendigt at implementere disse tiltag på trods af de barrierer, I oplevede?
- Hvilke positive konsekvenser har det haft for jeres virksomhed, at I har valgt at implementere tiltag, der har øget jeres IT-sikkerhed?
    a. Hvilke muligheder har det givet jer, at I har øget jeres IT-sikkerhed?
- Hvordan bruger I IT-sikkerhedstiltag i kommunikation til jeres kunder?
    a. Oplever I, at jeres kunder stiller krav til jeres IT-sikkerhed?
    b. Ser I muligheder i at øge jeres niveau af IT-sikkerhed ift. markedsføring mod jeres kunder (indenlandsk/udenlandsk)?
    c. Oplever I, at jeres leverandører og/eller andre samarbejdspartnere stiller krav til jeres IT-sikkerhed?
- Har I tidligere igangsat tiltag, som I var nødt til at udskyde eller helt stoppe?
    a. Hvilke tiltag er der tale om?
    b. Hvilke overvejelser gjorde I jer omkring at udskyde/stoppe tiltagene?
- Hvad har I overvejet af tiltag for at øge jeres IT-sikkerhed, men ikke implementeret?
    a. Hvilke tiltag er der tale om?
    b. Hvorfor valgte I ikke at gå videre med disse tiltag?
- Hvad kunne få jer til at implementere (flere) tiltag for at øge IT-sikkerheden i jeres virksomhed?
    a. Hvilke rammebetingelser (lovgivning og/eller regulering) ser I som nødvendige for at øge jeres IT-sikkerhed?

D. It-sikkerhed i en større kontekst

Til sidst vil vi gerne høre lidt mere om, hvordan I ser jeres IT-sikkerhed i fremtiden

- Hvordan forventer I at arbejde med IT-sikkerhed i fremtiden?
- Hvilke positive og negative konsekvenser ser I, jeres IT-sikkerhedsniveau kan få for jeres forretning i fremtiden?
- Hvordan forventer I, at jeres kunders krav til IT-sikkerhed vil ændre sig i fremtiden?
- Hvad er din generelle opfattelse af IT-sikkerheden i Danmark. (Brug nedenstående som uddybende spørgsmål)
    a. Hvordan ser du udviklingen inden for dette område?
    b. Ser du flere sikkerhedsbrud blandt jeres partnere/leverandører/kunder?
    c. Er det noget, der tales om i virksomhedens netværk blandt partnere/leverandører/kunder?

- Vi vil gerne bede om tilladelse til at bruge jeres virksomheds navn og logo i rapporten. Rapporten vil indeholde case-analyser af 15-20 virksomheder og ved at bruge virksomhedernes navn og logo, øges forståelsen for den enkelte case, konteksten samt giver bedre mulighed for at relatere casen til andre virksomheder i samme situation. Vi vil her gerne understrege, at vi naturligvis ikke offentliggør noget, uden I har set og godkendt materialet.

Dette var afslutningen på interviewet. Må vi kontakte dig igen, hvis vi har uddybende spørgsmål?

Erhvervsstyrelsen og Deloitte vil gerne takke dig for at deltage i denne undersøgelse. Dit input vil være afgørende for Erhvervsstyrelsens videre arbejde på dette område til gavn for danske virksomheder og landet som helhed.

Tak for hjælpen.

7.3.2 Udvælgelse af respondenter

Respondenterne til interviewene blev udvalgt på baggrund af fordelingen inden for arketyper, således interviewene er repræsentative for den samlede population. På denne måde er det muligt at lave antagelser om virksomhederne inden for de forskellige arketyper på baggrund af de kvalitative interviews.

Der blev udarbejdet en bruttoliste med virksomheder ud fra fordelingen inden for arketyperne. Virksomhederne på denne liste er udvalgt ud fra Deloitte Cyber Risks kendskab til virksomhedernes IT-sikkerhedsniveau og risikoprofil, således der blev foretaget en prækvalificering af virksomhederne.

7.3.3 Interviewforløb

Interviewene blev booket på forhånd med den relevante person i virksomheden for at sikre, at interviewpersonen tog sid til interviewet og gav fyldestgørende svar. Indledningsvist i hvert interview blev der gjort opmærksom på interviewets formål, samt at virksomheden potentielt ville blive brugt som case-virksomhed, hvis de gav samtykke til dette. Afslutningsvist blev der spurgt, om virksomheden ville give tilladelse til, at virksomheden figurerede med navn og logo i rapporten, hvis der kom relevant input i interviewet. Fem virksomheder gav foreløbig samtykke til, at deres virksomhed kunne fungere som case-virksomhed i indeværende rapport.

Interviewene blev primært foretaget med IT-ansvarlige i virksomhederne, hvilket kan have forvrænget resultaterne en anelse, da de IT-ansvarlige sandsynligvis ikke vil pege på dem selv som en del af udfordringen i IT-sikkerheden.

7.3.4 Dokumentation af interview

Ved hvert interview blev der spurgt om tilladelse til at optage interviewet til intern reference og dokumentation, hvilket alle virksomhederne indvilligede i. Derudover blev der taget noter under interviewet. Lydoptagelse samt noter blev brugt til at udarbejde et referat for alle interviews. Disse referater har dannet basis for at bygge de casebeskrivelser, der er brugt igennem rapporten samt de fulde casebeskrivelser i appendiks afsnit 7.4. Når en virk-

somhed nævnes med navn, har virksomheden godkendt indholdet og godkendt, at deres virksomhed beskrives med navns nævnelse.

7.4 Caseinterviews

Casefortegnelse:

- **Case 1:** Graf Design
- **Case 2:** Juhls Fabrik
- **Case 3:** Danmarks Naturfredningsforening
- **Case 4:** Sørensen Produktion
- **Case 5:** Secure Service
- **Case 6:** FinansieringNu
- **Case 7:** Fremtidens Læring
- **Case 8:** Maskinhandler Indkøbsringen
- **Case 9:** AB Hjem
- **Case 10:** Sund og Bælt
- **Case 11:** ToBu Transport
- **Case 12:** TP Aerospace
- **Case 13:** Blå Maritim
- **Case 14:** Aarhus Teater

7.4.1 **Case 1:** Graf Design (anonymiseret virksomhed – navnet er et alias)

Om virksomheden

Branche | Liberale, videnskabelige og tekniske tjenesteydelser

Størrelse | 30 medarbejdere

Arketype | Tilpas sikker

Virksomheden beskæftiger sig med kommunikation og branding

Virksomhedens IT-anvendelse

IT-sikkerhedsniveau | Middel

Risikoprofil | Middel

Virksomheden opbevarer data vedr. kundeopgaver, som er meget centrale for deres arbejde, da det er disse varer, de sælger. Hvis de mistede dette data, eller det blev lækket, vil de have store økonomiske konsekvenser for virksomheden, og de vil blive ramt på deres image. Derudover bruger virksomheden grafiske programmer til at udføre deres opgaver.

Introduktion til virksomhedens IT-sikkerhed

Virksomheden har valgt at udlicitere hele deres IT, da de har vurderet, at der er for lidt IT-relateret arbejde til at ansætte en intern IT-ansvarlig. Virksomheden bruger tre forskellige leverandører, som håndterer forskellige dele af deres IT, hvoraf den ene varetager det primære IT, og herunder er den, der varetager virksomhedens IT-sikkerhed. Denne leverandør besøger virksomheden en gang om ugen og løser diverse IT-relaterede problemer. Internt i virksomheden taler man om sund fornuft ift. IT-sikkerhed og har nedskrevne regler omkring f.eks. filhåndtering i deres medarbejderhåndbog, men der er ingen formaliseret træning af medarbejderne.

Virksomheden har aldrig oplevet et IT-sikkerhedsangreb eller IT-sikkerhedsbrud.

Oplevede drivere for at øge IT-sikkerhed

Hos denne virksomhed er det deres leverandør, der varetager IT-sikkerheden og ligeledes dem, der henvender sig med forslag til nye tiltag og produkter, som virksomheden diskuterer internt. Virksomheden har brugt denne leverandør i 20 år, og der er derfor opnået en tillid, der gør, at man stoler på, at leverandøren ikke bare kommer med relevante forslag og produkter, men også at de har kompetencerne til at løfte opgaven. Når man får et oplæg fra leverandøren, diskuterer man dette internt.

Derudover oplever virksomheden, at deres brug af en ekstern leverandør sikrer, at viden ikke går tabt. Havde man i stedet en intern IT-medarbejder, var der øget risiko forbundet med at miste denne viden, hvis medarbejderen skulle skifte job. Ved at bruge en ekstern leverandør håndterer de dette og kan give den relevante viden videre til interne medarbejdere.

Opmærksomheden omkring IT-sikkerhed i medierne er også noget, der gør, at man i virksomheden stopper op og overvejer, om ens egen IT-sikkerhed er tilstrækkelig. Da virksomheden dog har samarbejdet med den samme leverandør i flere år, har de ikke udfordret leverandøren, men sætter her sin lid til, at leverandøren har styr på IT-sikkerheden.

På nuværende tidspunkt oplever virksomheden ikke, at deres kunder direkte efterspørger IT-sikkerhed. Der stilles dog ofte krav til virksomhedens filhåndtering i de kontrakter, de har med deres kunder, idet kunderne ønsker, at virksomheden håndterer filerne sikkert internt.

Oplevede barrierer for at øge IT-sikkerhed

I og med at denne virksomhed har valgt at lægge al deres IT ud til deres leverandører, ligger eventuelle barrierer for arbejdet med IT-sikkerhed hos leverandøren, og det er derfor også dennes viden, kompetencer og arbejde, der kan være barrierer. Herunder kan leverandørens opmærksomhed mod den enkelte virksomhed og dennes IT-sikkerhed derfor være en barriere i det tilfælde, at leverandøren ikke har tilstrækkeligt fokus på virksomheden og dennes IT-brug, håndtering af data samt implementerede IT-sikkerhedsforanstaltninger.

Forventninger til fremtiden

Virksomheden forventer, at deres kunder vil stille større krav til IT-sikkerheden i fremtiden i takt med, at der kommer mere fokus på IT-sikkerhed generelt. Virksomheden ser dog, at de er godt med ift. IT-sikkerhed, men at de potentielt kan blive nødt til at lave opjusteringer for at kunne leve op til kundernes krav. Herunder have øget fokus på IT-sikkerhed i relation til medarbejderne, som virksomheden på nuværende tidspunkt ikke har haft fokus på.

Virksomheden siger selv:

"Det kræver meget tillid at lægge al sin IT og IT-sikkerhed ud til en ekstern partner, og man skal kunne stole på deres forslag til nye tiltag, og at disse er de rigtige for vores virksomhed. Vi har brugt leverandøren igennem mange år og har derfor opbygget den nødvendige tillid."

7.4.2 **Case 2:** Juhls Fabrik (anonymiseret virksomhed – navnet er et alias)

Om virksomheden

Navn | Juhls Fabrik

Branche | Fremstilling

Størrelse | ~250 medarbejdere

Arketype | Påpasselig

Juhls Fabrik er en dansk produktionsvirksomhed, der sælger til andre virksomheder

Virksomhedens IT-anvendelse

IT-sikkerhedsniveau | Høj

Risikoprofil | Høj

Virksomheden bruger IT til gængse ting som økonomistyring og personaledata. Derudover opbevarer Juhls Fabrik kritisk information om deres produkter. Derudover har Juhls Fabrik systemer, der bruges til overvågning i produktionen.

Introduktion til virksomhedens IT-sikkerhed

Juhls Fabrik har implementeret en række foranstaltninger for at øge deres IT-sikkerhed, herunder firewalls, antivirusprogrammer, patch management systemer og secure DNS. Derudover skal medarbejderne kontakte IT for at få lov til at installere software. Juhls Fabrik har samtidig segmenteret deres trådløse netværk i et administrativt netværk og et gæstenetværk, således man ikke får adgang til hele netværket i tilfælde af et IT-sikkerhedsbrud. Juhls Fabrik har en IT-politik, som alle medarbejdere skal skrive under på, og der er ligeledes lavet en test af medarbejdernes opmærksomhed over for phishingangreb ved at lave en Phishing Awareness Test. Denne gav et statusbillede af medarbejdernes opmærksomhed mod sådanne angreb, men den efterfølgende kommunikation omkring dette har også været med til at øge medarbejdernes viden og opmærksomhed. Fremadrettet vil Juhls Fabrik indføre follow-me print, og de planlægger ligeledes at lave mere central datahåndtering ved at have en server, hvor data gemmes på fremfor lokalt på medarbejdernes computere.

Juhls Fabrik har ikke oplevet et sikkerhedsbrud eller et forsøg herpå, men ser IT-sikkerhedstiltag som en forsikring, da det først er i det øjeblik, man oplever et angreb, at den får betydning. Juhls Fabrik opbevarer tegninger og patenter, som de har backup på, hvorfor de ikke frygter et ransomwareangreb, hvor data krypteres, fordi de ser, at de er forberedte på dette. Skulle det i stedet ske, at disse tegninger og patenter bliver lækket eller stjålet, kan det have kritisk betydning for Juhls Fabriks forretning.

Oplevede drivere for at øge IT-sikkerhed

Den primære driver for at øge IT-sikkerheden hos Juhls Fabrik har været Juhls Fabriks IT-managers interesse i IT-sikkerhed og ambition om at øge denne i virksomheden. Dernæst har en driver været en større viden om IT-sikkerhedstrusler og muligheder for at øge IT-sikkerheden, både hos den IT-sikkerhedsansvarlige, men også hos ledelsen og de resterende medarbejdere. Denne øgede viden på tværs af organisationen er bl.a. opnået ved brug af en ekstern Cyber Risk rådgiver, der kortlagde, hvor sikkerhedstruslen var størst hos Juhls Fabrik. Den IT-ansvarlige bestilte denne analyse og oplevede, at den var et godt kommunikationsværktøj internt i organisationen efterfølgende til at oplyse om virksomhedens huller i IT-sikkerheden.

Juhls Fabrik er vokset de senere år, hvilket har betydet flere ressourcer til IT, og dette har frigivet ressourcer til at prioritere IT-sikkerhed i højere grad.

Oplevede barrierer for at øge IT-sikkerhed

I Juhls Fabriks arbejde med at øge IT-sikkerhedsniveauet har den primære barriere været manglende viden om IT-sikkerhed og potentielle konsekvenser ved manglende IT-sikkerhed både hos medarbejdere og ledelse. Grundet den manglende viden om IT-sikkerhed, blev det ikke prioriteret, og der blev således ikke allokeret ressourcer til at øge IT-sikkerheden. Det har været en nødvendighed for den IT-ansvarlige at forklare til ledelsen hvilke konsekvenser, et IT-sikkerhedsbrud kan medføre, for at ledelsen ville frigive de nødvendige ressourcer til at arbejde med IT-

sikkerhed. Det har dog også været centralt at kommunikere det til medarbejderne og få deres accept, da de har følt sig mere begrænsede i deres færden på internettet med de nye tiltag.

En barriere for den fremtidige indsats er fortsat begrænset viden, både om de sikkerhedstrusler, der er, men også de IT-sikkerhedsmuligheder, der er på markedet. Juhls Fabrik holder sig opdateret ved selv at opsøge viden på internettet og ved at modtage viden gennem nyhedsbreve om emnet. Virksomheden finder dog, at det kan være svært at navigere i hvilke produkter og muligheder, der er på markedet.

Forventninger til fremtiden

IT-manageren hos Juhls Fabrik ser trusselsbilledet som støt stigende og forventer derfor også, at det kræver en yderligere forøgelse af IT-sikkerheden i Juhls Fabrik, bl.a. ved bedre uddannelse af medarbejderne. Ligeledes forventer han, at de i virksomheden i højere grad vil komme til at tale med leverandører om IT-sikkerhed, og at dette vil være noget, der bliver en del af deres vurdering af leverandører. For nuværende laver Juhls Fabrik sikkerhedsbesøg hos leverandørerne, og han forventer, at IT-sikkerhed på sigt bliver en del af dette, men ved også, at dette kræver bedre uddannelse af de medarbejdere, der laver disse besøg, men samtidig også en bedre dialog om dette med leverandørerne.

Virksomheden siger selv:

"IT-sikkerhed er som en forsikring – den bliver først vigtig i det øjeblik, man oplever et angreb. Derfor kan det være svært at overbevise ledelsen om den økonomiske gevinst, da man ikke umiddelbart kan forudsige, hvornår denne vil opstå og i så fald, hvad den vil være."

7.4.3 Case 3: Danmarks Naturfredningsforening

Om virksomheden

Navn | Danmarks Naturfredningsforening

Branche | Offentlig forvaltning og forsvar

Størrelse | 70 medarbejdere

Arketype | Tilpas sikker

Danmarks Naturfredningsforening er en forening, der arbejder for at bevare landskabet og naturen i Danmark.

Virksomhedens IT-anvendelse

IT-sikkerhedsniveau | Middel

Risikoprofil | Middel

Virksomheden opbevarer data om deres medlemmer, herunder adresse og CPR-numre, men ikke noget, der er særlig personfølsomt. Denne data er dog vigtig for forretningen, da det udgør deres finansieringsgrundlag. De har et medlemssystem til at håndtere dette, hvor data opbevares.

Introduktion til virksomhedens IT-sikkerhed

Danmarks Naturfredningsforening har outsourcet størstedelen af deres IT til en ekstern leverandør, som hoster deres servere. Virksomheden har valgt leverandøren, fordi de på baggrund af leverandørens andre kunder og leverandørens ISO-certificering kunne se, at IT-sikkerheden var god, og at deres data derfor var beskyttet. Man valgte at udlicitere, fordi IT kræver mange fagligheder, og virksomheden havde ikke alle de nødvendige kompetencer internt.

Hos Danmarks Naturfredningsforening tager man backup af dokumenter, men i særlig grad også medlemsdata. Derudover har man filtre på alle emailsystemerne for at undgå spammails. Virksomheden har også tilkøbt diverse produkter fra deres leverandør, herunder produkter, der scanner de enkelte medarbejderes computere. Virksomheden har udover de tekniske foranstaltninger også haft fokus på medarbejderne, hvor man bl.a. har lavet en phishing-test. Udover denne test sørger man også for løbende at kommunikere til medarbejderne omkring IT-sikkerhed, f.eks. gennem interne oplæg, i tilfælde af sager i medierne og har udarbejdet en folder.

Virksomheden får løbende information omkring IT-sikkerhed og IT-trusselsbilledet gennem deres leverandør. Derudover følger de også med i medierne om, hvad der rører sig på området, og hvordan udviklingen går.

Danmarks Naturfredningsforening har for et par år tilbage oplevet et IT-sikkerhedsangreb i form af et ransomware-angreb, hvor filerne blev låst, som de hurtigt fik styr på vha. backup, således, at det ikke fik nogle konsekvenser for virksomheden. Virksomheden havde implementeret backup, da de for over 10 år siden havde et IT-systemnedbrud, hvor de mistede en del medlemsdata. De fik genskabt data ved at samle information rundt omkring fra medarbejdernes filer på computerne. Dette betød, at virksomheden identificerede, at medlemssystemet var særlig kritisk for deres forretning, da det opbevarede det vigtigste data. Derfor sørgede man efterfølgende for at have backup af sin data for ikke at stå i samme situation på et senere tidspunkt.

Oplevede drivere for at øge IT-sikkerhed

Der ligger flere overvejelser bag Danmarks Naturfredningsforenings arbejde med IT-sikkerhed.

For det første har de nogle år tilbage oplevet et IT-sikkerhedsangreb i form af et ransomware-angreb, hvor de fik deres filer låst, men virksomheden kunne løse dette efter 10 min, fordi de havde taget de nødvendige forbehold, herunder implementeret backup. Dette IT-sikkerhedsangreb fik dog virksomheden til at øge fokus endnu mere på IT-sikkerhed, således de kunne sikre sig mod eventuelle fremtidige angreb. Derudover har det betydet, at der er kommet større fokus på IT-sikkerhed internt i virksomheden blandt medarbejdere og ledelsen.

For det andet har Danmarks Naturfredningsforening haft et ønske om at sikre IT-driften for deres medlemmer, hvorfor de har intensiveret deres fokus på IT-sikkerhed. Hvis de oplevede angreb hele tiden, vil det være forstyrrende for deres arbejde, da medarbejderne ikke vil kunne arbejde. De oplever, at fordi trusselsbilledet stiger, kræver det, at man fortsætter indsatsen for fortsat at være beskyttet.

Oplevede barrierer for at øge IT-sikkerhed

Medarbejdernes ageren og færden på nettet har været den største barriere for at øge IT-sikkerheden i Danmarks Naturfredningsforening. Medarbejderne er det svageste led, da de kan komme til at klikke på et link eller en fil i en mail, som slipper gennem filteret, og man oplever, at det kræver meget fokus på forandringsledelse, således fokus på IT forankres i kulturen og arbejdsgange. Der er stor fokus på kommunikation omkring IT-sikkerhed, og medarbejderne er meget interesserede og spørger også selv ind til råd i specifikke situationer. Man har kørt en phishing-test, som udover at teste niveauet for IT-sikkerhed i virksomheden, også var med til at øge fokus på IT-sikkerhed blandt medarbejderne, da det skabte en forståelse for, hvordan en phishingmail kan se ud og hvor nemt, man kan falde i. Kommunikationen er vurderet som central for IT-sikkerheden, og da den IT-ansvarlige er uddannet inden for kommunikation er han i stand til at lave særlige og målrettet kommunikationsindsatser.

Hos Danmarks Naturfredningsforening søger man hele tiden at afveje nødvendigheden af de produkter, som deres leverandør tilbyder, da de ser, at visse produkter vil være for komplekse til deres behov. Sådanne produkter vil forstyrre deres arbejde for meget ift., hvad det vil betyde for deres IT-sikkerhed, hvorfor man vælger ikke at benytte sig af disse produkter.

Forventninger til fremtiden

Man vil hos Danmarks Naturfredningsforening fortsætte sit arbejde med IT-sikkerhed for at søge at følge med den udvikling, der sker på området, og man har bl.a. i pipeline at indføre et intern 2-faktorsystem på deres medlemsdata. De ser, at deres medlemmer muligvis også vil komme til at stille større krav til IT-sikkerhed, fordi der kommer mere fokus på IT-sikkerhed i det offentlige, og særligt hvis man på foreningsområdet vil se et brud eller angreb på et tidspunkt. De vil fortsat stille krav til deres leverandør og derudover holde fokus på at informere medarbejderne.

Virksomheden siger selv:

"Vi har øget IT-sikkerheden for at sikre driften. Hvis man har et angreb en gang om ugen, der lægger ens IT ned, kan man ikke drive virksomhed."

7.4.4 **Case 4:** Sørensen Produktion (anonymiseret virksomhed – navnet er et alias)

Om virksomheden

Navn | Sørensen Produktion

Branche | Industri

Størrelse | 10-19 medarbejdere

Arketype | Tilpas sikker

Virksomheden producerer trævarer, hvor de blandt andet genanvender træ

Virksomhedens IT-anvendelse

IT-sikkerhedsniveau | Middel

Risikoprofil | Middel

Virksomheden opbevarer kundedata i et CRM-system, hvor de dokumenterer interaktion med kunderne samt opbevarer kontrakter og kundeoplysninger og –historik. Derudover har virksomheden et ERP-system og ligeledes et system, der bruges til at planlægge produktionen, og produktionen kræver adgang til IT for at kunne køre.

Introduktion til virksomhedens IT-sikkerhed

Sørensen Produktion har outsourcet hele sin IT og har således intet IT internt. Det betyder, at de har computere i virksomheden, men servere osv. ligger centralt hos deres leverandør. Det valgte virksomheden at gøre, fordi de mente, de ikke havde de nødvendige kompetencer og ressourcer internt, herunder evnen til selv at varetage IT-sikkerhed.

De foranstaltninger, der er lavet i relation til Sørensen Produktions IT-sikkerhed, er backup, løbende opdatering af systemer, password på computere og dobbelt kontrol ved brug af computer uden for virksomhedens kontor samt lukket brugeradgang til specifikke dele af virksomhedens data og systemer. Internt i virksomheden forsøger man at kommunikere sund fornuft til medarbejderne, og derudover har man årligt besøg af en ekspert fra virksomhedens forsikringsselskab, som bl.a. fortæller om IT-sikkerhed. Derudover har man i virksomheden en intern regel om, at man ikke må gemme private filer på arbejdscomputerne for derved at holde det private IT-brug adskilt fra det arbejdsrelaterede IT-brug og derved undgå at få f.eks. malware gennem private filer.

Virksomheden får størstedelen af deres viden om IT-sikkerhed fra deres leverandør og derudover igennem netværk og andre kontakter, hvor man erfaringsdeler, bl.a. om konsekvenserne, eventuelle brud kan have.

Sørensen Produktion har oplevet et IT-angreb af typen direktørsvindel, hvor direktørens mail var blevet hacket, og der blev sendt en mail til regnskabschefen, hvor der blev bedt om at overføre en sum penge til en konto. Mailen virkede meget troværdig, især fordi den kom fra en intern mailadresse.

Oplevede drivere for at øge IT-sikkerhed

Den primære driver for Sørensen Produktions IT-sikkerhed er deres leverandør, som varetager al deres IT. Her henvender leverandøren sig til virksomheden, hvis der skal ske nogle ændringer, og så forholder Sørensen Produktion sig til det.

Derudover har Sørensen Produktion efter deres oplevelse med forsøg på direktørsvindel, valgt at ændre nogle sikkerhedsprocedurer, således man ikke vil kunne overføre større summer af penge uden særlig godkendelse. Der skal bl.a. altid være en mundtlig godkendelse fra personen, der anmoder om en pengeoverførsel for at sikre, at anmodningen faktisk kommer fra denne person. Virksomheden har ligeledes oplevet, at en tidligere IT-leverandør mistede en del af virksomhedens data, hvorfor man valgte at skifte leverandør, fordi man ikke længere følte, at man kunne stole på denne leverandør. Her brugte man sit netværk til at identificere en ny leverandør.

Oplevede barrierer for at øge IT-sikkerhed

Da Sørensen Produktion har valgt at outsource hele sin IT, er der ingen IT-ansvarlige i huset, og Sørensen Produktion oplever, at det kan være en udfordring i relation til IT-sikkerheden, da de ikke har den nødvendige viden og de nødvendige kompetencer til at kunne se, om deres leverandør har en tilstrækkelig IT-sikkerhed. De ser derfor, at

den største usikkerhed ift. IT-sikkerhed for dem er, om deres samarbejdspartner er dygtig nok. Sørensen Produktion oplever generelt, at IT-leverandørerne i kontrakterne fraskriver sig ansvaret, men at de altid beretter om alle de gode ting, de har indført ift. IT-sikkerhed. Sørensen Produktion ser derfor, at de er nødt til at stole på, at leverandøren kan levere på det, de siger, da virksomheden ikke selv har tilstrækkelig med viden til at vide, om de kan.

Forventninger til fremtiden

Sørensen Produktion oplever ikke på nuværende tidspunkt, at deres kunder efterspørger IT-sikkerhed og har krav til dette. Virksomheden oplever dog, at der i mange kontrakter med kunder er mange paragraffer vedr. f.eks. underleverandører og materialer, og man forestiller sig, at dette på sigt også vil komme til at vedrøre IT-sikkerhed.

Virksomheden siger selv:

"Vi har ikke tilstrækkelig med viden til at kunne se, om leverandøren har tilstrækkelig med IT-sikkerhed. Det er den største usikkerhed, om samarbejdspartneren er dygtig nok."

7.4.5 **Case 5:** Secure Service (anonymiseret virksomhed – navnet er et alias)

Om virksomheden

Navn | Secure Service

Branche | Andre serviceydelser

Størrelse | 50-99 medarbejdere

Arketype | Tilpas sikker

Secure Service sælger IT-løsninger til andre virksomheder.

Virksomhedens IT-anvendelse

IT-sikkerhedsniveau | Høj

Risikoprofil | Høj

Secure Service opbevarer data for sine kunder, som kan være af personfølsom karakter på kundernes kunder. De har derudover nogle særlige systemer, som de bruger i deres forretning, og beskrivelserne af dem er centrale for forretningen, og et læk af disse vil være kritisk.

Introduktion til virksomhedens IT-sikkerhed

Hos Secure Service har de en dokumenteret IT-sikkerhedspolitik, som de reviderer en gang om året, og som godkendes af deres bestyrelse. Denne sikkerhedspolitik operationaliseres ned i en række rammekrav og ender til sidst ud i specifikke proceskrav. Secure Service får lavet en 3402-erklæring, dvs. en revisorerklæring af, at virksomheden har ordentlige IT-forhold, og at de lever op til lovkrav. Derudover har Secure Service valgt at få foretaget en IT-revision en gang om året, hvor de får vurderet deres IT-sikkerhedsniveau. I relation til dette får Secure Service også foretaget forskellige tests, f.eks. en penetrationstest, af eksterne sikkerhedsfirmaer for at teste sikkerheden i deres IT. Secure Service har derudover haft enkelte medarbejdere på kurser relateret til IT-sikkerhed. Ligeledes tager Secure Service backup af deres data, har begrænset adgang til serverrum, og de har derudover også firewallsystemer til at spore, hvad der sker i deres systemer.

Secure Service bruger i høj grad de revisorer, der foretager deres IT-revision samt andre samarbejdspartnere, til at få ny information og viden og sparre omkring, hvad der giver mening for Secure Service at implementere af IT-sikkerhedstiltag. Derudover deltager de i forskellige konferencer og messer om IT-sikkerhed. Her får de viden om, hvad der er af nye produkter, hvilke IT-sikkerhedstrusler man ser i øjeblikket, samt omkring håndtering af medarbejdere, hvor der er fokus på forandringsledelse.

Secure Service har oplevet at blive angrebet med ransomware tre gange. Alle gangene har de kunne iværksætte de procedurer, de har på området, og de har således ikke lidt noget tab eller været nødsaget til at betale en løsesum for deres data. De har kunne bruge deres firewallsystemer til at identificere, hvordan angrebet er kommet ind, og på den måde har de kunne isolere det og bruge deres backup til at gendanne data og således fjerne det ransomware, de er blevet ramt af. Det tog Secure Service lidt tid at komme helt til bunds, men de oplevede, at de procedurer, de havde på området, gjorde dem i stand til at behandle IT-sikkerhedsangrebet, uden det fik konsekvenser for virksomhedens drift eller deres kunder. Skulle der være et læk af data, vil dette have store konsekvenser for virksomheden og dens kunder, og det kan betyde, at virksomhedens image skades, og at de dermed mister kommercielle muligheder.

Oplevede drivere for at øge IT-sikkerhed

Regulering på området har været en stor driver for Secure Services arbejde med IT-sikkerhed. Herunder har den nye persondataforordning haft stor betydning og været med til i højere grad at sætte IT-sikkerhed på agendaen blandt ledelsen, da der nu er risiko for at få en bøde, hvis man ikke opfylder kravene. Her er den økonomiske risiko en driver for Secure Service til at øge IT-sikkerheden, men det er i højere grad også det imagetab, der kan være ved ikke at overholde persondataforordningen og dermed risikoen for at miste kunder. Persondataforordningen har også været medvirkende til, at ledelsen forsøger at sætte sig mere ind i tingene og selv opnå en større viden om tingene og samtidig også betydet, at det er noget, ledelsen vælger at prioritere.

Secure Service bruger deres arbejde med IT-sikkerhed i kommunikationen mod deres kunder og ser det som en salgsparameter. Derfor deler de også deres 3402-erklæring med deres kunder, så kunderne kan se, hvad Secure

Service er blevet revideret på. Derudover deler Secure Service deres tiltag med kunderne samt planer for, hvad de vil iværksætte for på den måde at inspirere deres kunder til at lave lignende tiltag. I og med at manglende IT-sikkerhed kan påvirke Secure Services image over for kunderne, ønsker Secure Service i høj grad at formidle, hvordan de arbejder med dette samt vise, at deres arbejde har fået et blåstempel af eksterne revisorer.

Oplevede barrierer for at øge IT-sikkerhed

En barriere for Secure Service har for den IT-ansvarlige været at italesætte emnet over for ledelsen. IT og IT-sikkerhed kan være et komplekst område at formidle, og det har derfor til tider været svært at gøre det håndgribeligt og ikke mindst sætte det i en forretningsmæssig kontekst. I den relation har IT-revisionerne dog spillet ind, da IT-afdelingen har kunne bruge disse til at udpege de eventuelle huller, der kan være, og det har gjort det nemmere at nå igennem med, når det kommer fra en ekstern aktør. Det letter den kommunikative opgave og har gjort, at i stedet for at IT-afdelingen skal igangsætte det, accepterer ledelsen fra starten, at der skal implementeres noget og henvender sig til IT for at finde ud af, hvad man skal gøre.

I arbejdet med at øge IT-sikkerhed har beslutningsprocessen også vist sig at være en barriere, da den til tider kan være langsommelig. Selvom ledelsen har fået mere fokus på IT-sikkerhed, prioriterer de nogle gange forretningsrelaterede beslutninger højere og udskyder dermed beslutninger på IT-sikkerhed.

Hos Secure Service er mange medarbejdere meget IT-kyndige. Til trods for det oplever de, at medarbejderne til tider kan være en hindring i arbejdet, da der kan være en følelse af, at de ved bedst og godt kender til dette. I deres arbejde forsøger Secure Service derfor at implementere tiltag, som medarbejderne er nødt til at følge, da der kan være en organisatorisk modstand mod disse forandringer, og medarbejderne vil måske forsøge at omgå det. Derudover laver Secure Service ved større IT-sikkerhedstiltag arbejdsgrupper, så alle afdelinger i huset bliver hørt og samtidig kan fungere som interne ambassadører for tiltaget. Derudover arbejder Secure Service med at italesætte det over for medarbejderne, ift. hvorfor det er nødvendigt, hvad der skal ske, og hvilken betydning det får for dem og deres arbejde med det formål at reducere medarbejdernes modvillighed mod disse tiltag.

Secure Service har oplevet, at de har været nødt til at udskyde IT-sikkerhedstiltag til et senere tidspunkt. Dels pga. økonomi og ressourcemangel, men også fordi Secure Service ikke har de nødvendige kompetencer til at løfte opgaven. Secure Service har bevidst valgt ikke at bruge konsulenter og få disse kompetencer fra et eksternt sted, da de ser det som problematisk, at de så kun har disse kompetencer til rådighed i en periode, og de ønsker i højere grad at søge at tilegne sig denne viden internt.

Forventninger til fremtiden

Secure Service vil i fremtiden arbejde mere med at træne medarbejderne i IT-sikkerhed og lave awareness-træning for at øge medarbejdernes bevidsthed omkring IT-sikkerhed samt italesætte emnet endnu mere.

Virksomheden forventer, at der fra kundernes side vil komme et øget krav til IT-sikkerhed. De ser, at persondataforordningen har speedet processen omkring IT-sikkerhed op og har drevet meget opmærksomhed mod emnet. Det har også medført, at kunderne er mere opmærksomme på det, og Secure Service forventer, at denne udvikling kun vil fortsætte. Derfor regner de også med, at det er et område, der vil kræve flere ressourcer i fremtiden, både økonomisk, men også på mandskab. Det vil kunne bruges som en konkurrenceparameter både til at fastholde eksisterende kunder, men også som en salgsparameter til at tiltrække nye kunder.

Virksomheden siger selv:

"Persondataforordningen har gjort, at ledelsen nu er mere opmærksomme på IT-sikkerhed og prioriterer det, både økonomisk og ressourcemæssigt. Det starter med et økonomisk perspektiv for at undgå bøder, men det øger også fokus og viden."

7.4.6 **Case 6:** FinansieringNu (anonymiseret virksomhed – navnet er et alias)

Om virksomheden

Navn | FinansieringNu

Branche | Pengeinstitut og finansvirksomhed

Størrelse | 40 ansatte

Arketype | Tilpas sikker

Virksomheden støtter andre virksomheder i finansiering af f.eks. erhvervslokaler

Virksomhedens IT-anvendelse

IT-sikkerhedsniveau | Middel

Risikoprofil | Middel

FinansieringNu opbevarer data om kunder, herunder finansieringshistorik. Herudover anvender virksomheden et administrationssystem, som medarbejderne bruger i deres daglige arbejde.

Introduktion til virksomhedens IT-sikkerhed

Hos FinansieringNu har man et administrationssystem af ældre dato, som man er i gang med at udskifte. Herudover har man krypteret alle bærbare computere, således at hvis de skulle falde i de forkerte hænder, vil man ikke kunne få adgang til filer, der ligger på computerne. Generelt har man arbejdet med de grundlæggende tekniske foranstaltninger, herunder firewall og sikre passwords. Man har internt haft meget fokus på at skabe opmærksomhed blandt medarbejderne, bl.a. gennem deres månedsmøder og derudover forsøger man at gøre IT-sikkerhed sjovere ved at bruge anekdoter, f.eks. omkring hvordan det ikke hjælper at have et stærkt password, hvis man har en post-it med passwordet klistret på sin computer og lignende.

Virksomheden har valgt at outsource en del af deres IT, fordi de ser, at de ikke har de tilstrækkelige kompetencer internt til at varetage de opgaver, de har outsourcet. De er dog også i proces omkring at insource elementer af driften igen, fordi de ønsker nemmere at kunne ændre ting selv.

Viden omkring IT-sikkerhed får den IT-ansvarlige gennem diverse netværk og fora og forsøger at holde sig opdaterede ved at følge med i udviklingen.

Oplevede drivere for at øge IT-sikkerhed

FinansieringNu oplever, at deres IT-sikkerhed øges, fordi de har valgt at outsource dele af deres IT. De ved, at de ikke selv har tilstrækkelige evner, og da det ikke er nok kun at være 80% gode til IT-sikkerhed, oplever de, at det øger deres IT-sikkerhed at bruge outsourcing. En anden driver for virksomhedens arbejde med IT-sikkerhed er, at de ser, at trusselsbilledet hele tiden stiger, og at de har noget data, som de ikke vil miste, hvorfor de er nødt til at øge IT-sikkerheden ved i særlig grad at fokusere på IT-sikkerhed internt blandt medarbejderne.

Virksomheden ser, at der er meget fokus på IT-sikkerhedsbrud i medierne, f.eks. ift. Mærsk, og det gør, at det er nemmere at overtale ledelse og medarbejdere, og det betyder også, at man kan sætte IT-sikkerhed i en kontekst og dermed gøre det mere håndgribeligt.

Oplevede barrierer for at øge IT-sikkerhed

FinansieringNu ser, at økonomi nogle gange kan være en barriere for IT-sikkerhed, fordi IT-sikkerhed kræver mange ressourcer, og derfor er man nogle gange nødt til at prioritere anderledes. Tidligere brugte man flest penge på udvikling, men i dag ser FinansieringNu, at IT-sikkerhed kræver en større del af budgettet, og det betyder, at det kan være sværere at få pengene til det.

Derudover ser FinansieringNu, at medarbejdernes opmærksomhed nogle gange kan være en barriere, fordi man frygter, at man sender for meget information deres vej. Hvis man hele tiden sender de samme typer information ud, lytter medarbejderne ikke længere, fordi de føler, at de har hørt denne information og ved det. Man frygter, at medarbejderne bliver trætte af at høre om IT-sikkerhed og derfor lukker af for informationen.

Forventninger til fremtiden

Hos FinansieringNu oplever man ikke, at kunder stiller spørgsmål til IT-sikkerhed, men man håber, at de bliver mere opmærksomme på det i fremtiden, for at man også i højere grad kan øge sikkerheden hos dem.

7.4.7 **Case 7:** Fremtidens Læring (anonymiseret virksomhed – navnet er et alias)

Om virksomheden

Navn | Fremtidens Læring

Branche | Administrative tjenesteydelser og hjælpetjenester

Størrelse | 100-249 medarbejdere

Arketype | Tilpas sikker

Virksomhederne er en faglig virksomhed, der bl.a. udbyder diverse kurser.

Virksomhedens IT-anvendelse

IT-sikkerhedsniveau | Høj

Risikoprofil | Høj

Virksomheden opbevarer oplysninger om deres kunder, og de anvender et IT-system, som håndterer dette. Samtidig har virksomheden gængse systemer som økonomisystem.

Introduktion til virksomhedens IT-sikkerhed

Hos Fremtidens Læring har man en dokumenteret IT-sikkerhedspolitik, som gennemgås en gang om året. Denne baseres på ISO 27001, og derfor er Fremtidens Lærings tilgang til IT-sikkerhed baseret på risikovurderinger. Dette betyder, at hver gang man et sted i forretningen ønsker at implementere et nyt IT-sikkerhedstiltag, så vejer man omkostningerne ved tiltaget op mod de potentielle risici, dette kan medføre. Dette gør man ved at gennemgå 6-8 prædefinerede spørgsmål, som afdækker risiciene, som det pågældende tiltag vil mitigere. Ligeledes har Fremtidens Læring lavet tiltag direkte målrettet deres medarbejdere, hvor de kører interne awareness-kampagner. Der er også lavet en introduktionsvideo til nye medarbejdere omkring, hvordan man agerer, når man anvender IT. Derudover får Fremtidens Læring lavet eksterne sårbarhedsanalyser til at vurdere, hvor der er huller i deres sikkerhed, således de har mulighed for at rette op på dette. Fremtidens Læring har udliciteret drift af deres kritiske IT-systemer til en ekstern host.

Viden omkring IT-sikkerhed og trusler får man ved Fremtidens Læring igennem samarbejdspartnere på området, og derudover abonnerer virksomheden på forskellige tjenester, hvor man får information om, hvad der rører sig.

Fremtidens Læring har oplevet mindre sikkerhedsbrud, f.eks. direktørsvindel, hvor de dermed betalte nogle penge, de ikke skulle. Dog havde virksomheden en forsikring mod dette, som dækkede størstedelen af tabet.

Oplevede drivere for at øge IT-sikkerhed

Den primære driver for Fremtidens Lærings arbejde med IT-sikkerhed har været, at der skal være styr på IT-sikkerhed, fordi de håndterer personfølsomme data på vegne af deres kunder. Dette for at tilsikre, at kunderne opfatter dem som troværdige og er trygge ved at give dem deres oplysninger. Direktionen i Fremtidens Læring står derfor også bag denne agenda og prioriterer IT-sikkerhed.

Fremtidens Læring har oplevet mindre IT-sikkerhedsbrud, og disse har betydet, at de har iværksat tiltag målrettet disse typer af IT-sikkerhedsangreb. Det har betydet, at der er blevet ændret på visse procedurer og arbejdsgange, således man ikke er ligeså sårbar over for disse typer af IT-sikkerhedsangreb. Det har derudover også været med til at øge fokus på IT-sikkerhed over for medarbejdere og gjort det muligt bedre at kunne sætte IT-sikkerhed i en håndgribelig kontekst.

Derudover har Fremtidens Læring oplevet, at kunder på deres kursusfaciliteter har efterspurgt, at det er vigtigt, at data omkring de kurser, de deltager på og indholdet, er sikret, og her har Fremtidens Læring kunne leve op til forventninger om datakryptering.

Oplevede barrierer for at øge IT-sikkerhed

Hos Fremtidens Læring oplever man, at medarbejdernes handlinger og manglende viden om IT-sikkerhed kan være en barriere i arbejdet med IT-sikkerhed, især fordi størstedelen af medarbejderne også bruger IT i det private, og

det kan være svært at forklare, hvordan man skal agere forskelligt, når man håndterer IT professionelt og privat. Professionelt kan det have større konsekvenser, hvis man bliver udsat for et IT-sikkerhedsbrud. Her forsøger man hos Fremtidens Læring i høj grad at tale med medarbejderne om det, skubbe information ud til dem og give dem værktøjer til, hvordan de kan sikre IT-sikkerhed i deres arbejde. I denne kommunikation benytter virksomheden sig også af eksempler fra medierne, hvor virksomheder har oplevet et IT-sikkerhedsbrud.

Derudover oplever den IT-ansvarlige hos Fremtidens Læring, at det kan være svært at kommunikere IT-sikkerhed i en håndgribelig kontekst over for ledelsen, da det kræver, at man kan formulere noget meget teknisk på en mere håndgribelig og konkret måde, der gør det lettere at forstå for personer, der ikke har en IT-baggrund.

I en virksomhed hvor man er nødt til at prioritere sine ressourcer, har Fremtidens Læring også til tider været nødt til at udskyde tiltag på IT-sikkerhedsområdet, fordi der ikke var ressourcer eller kompetencer til at varetage opgaven.

Forventninger til fremtiden

Hos Fremtidens Læring forventer man, at i takt med at verden ændrer sig, og man ser mere automation og f.eks. robotics, vil det også kræve mere af IT-sikkerheden, som skal tilpasses disse forandringer. Det kræver, at man simultant kigger på, hvad sådanne nye tiltag kræver af ændringer på IT-sikkerheden, således man mindsker sine risici. Det handler om at være på forkant og handle proaktivt.

Derudover forventer man hos Fremtidens Læring, at man på sigt vil opleve større krav fra kunderne ift. IT-sikkerhed.

7.4.8 **Case 8:** Maskinhandler Indkøbsringen

Om virksomheden

Navn | Maskinhandler Indkøbsringen

Branche | Engroshandel og detailhandel

Størrelse | 65 medarbejdere

Arketype | Påpasselig

Virksomheden er et indkøbssamarbejde mellem danske maskinforretninger, som sælger maskiner til private og erhverv

Virksomhedens IT-anvendelse

Modenhedsniveau | Middel

Risikoprofil | Lav

Virksomheden lagrer data vedr. kunder, herunder ordrer samt login til webside, og derudover information omkring leverandører og derudover personaledata

Introduktion til virksomhedens IT-sikkerhed

Maskinhandler Indkøbsringen er for nyligt begyndt at have fokus på deres IT-sikkerhed og er derfor midt i processen med at øge deres IT-sikkerhed. Man havde i virksomheden været opmærksom på, at man havde behov for en højere grad af IT-sikkerhed og efter et seminar, hvor en ekstern rådgiver fortalte om IT-sikkerhed, fik man denne ekstern rådgiver til at lave en IT-sikkerhedsanalyse. Herefter påbegyndte man arbejdet med at øge IT-sikkerheden på baggrund af de anbefalinger og den viden, man fik fra den eksterne partner. Man har derudover indgået en treårig aftale med denne partner, således man får testet IT-sikkerheden årligt i tre år. Analysen har givet Maskinhandler Indkøbsringen anledning til at påbegynde arbejdet med IT-sikkerhed internt, og man er ligeledes i dialog med andre partnere, som skal hjælpe virksomheden med at implementere forskellige IT-sikkerhedsforanstaltninger. I relation til medarbejderne forsøger man at kommunikere IT-sikkerhed bl.a. ved at bruge eksempler på phishing-mails, og man prøver derudover at skabe et miljø, hvor man gerne må spørge IT-afdelingen om hjælp, hvis man er i tvivl.

Virksomheden er i gang med at skabe overblik over virksomhedens data for at vurdere hvor personfølsomt, dette data er, da man både skal vurdere hvor kritisk, data er, men ligeledes også for at være i stand til at vurdere dette data ift. persondataforordningen, så man kan sikre, man handler i overensstemmelse med dette.

Maskinhandler Indkøbsringen har størstedelen af deres IT internt, men har outsourcet enkelte elementer. Man har valgt at beholde serverne internt, som står aflåst sted, hvor kun personer fra IT-afdelingen har adgang til.

Hos Maskinhandler Indkøbsringen oplever man mange phishingmails, men har endnu ikke oplevet et angreb, der har givet anledning til et egentlig sikkerhedsbrud. Man har oplevet, at en bruger fik klikket på en phishing-mail, men her fik man hurtigt slukket for maskinen og serverne, således det ingen konsekvenser fik.

Viden omkring IT-sikkerhed får man ved Maskinhandler Indkøbsringen primært fra faglige medier, og man bruger derudover det sociale medie Twitter, hvor man kan få opdateringer om hvilke IT-sikkerhedstrusler, der er lige nu. Virksomheden ser, at udover det er nemt, får man også informationen i realtid.

Oplevede drivere for at øge IT-sikkerhed

Det der startede Maskinhandler Indkøbsringens arbejde med IT-sikkerhed var et IT-seminar med ekstern rådgivningsvirksomhed. På baggrund af dette valgte Maskinhandler Indkøbsringen at få foretaget en IT-sikkerhedsanalyse. Det gav et overblik over, hvad der manglede ift. IT-sikkerhed og hvilke tiltag, man kunne implementere for at øge IT-sikkerheden i virksomheden. Derudover kunne man bringe resultaterne fra analysen til ledelsen i virksomheden, og man oplevede, at det hjalp, at man kunne kommunikere tingene fra et eksternt perspektiv. Man fik i denne henseende den eksterne rådgiver til at komme og præsentere resultaterne for ledelsen, og dette betød, at det blev nemmere at få de nødvendige ressourcer til at øge IT-sikkerheden af ledelsen. Ligeledes ser man hos Maskinhandler Indkøbsringen, at det har stor værdi, at der er kommet mere fokus på IT-sikkerhed i medierne, da også øger fokus og forståelse generelt i virksomheden.

Man oplever hos Maskinhandler Indkøbsringen, at der kommer mange phishing-mails, og det er både forstyrrende for medarbejdernes arbejde og risikofyldt, hvis medarbejderne i et uopmærksomt øjeblik klikker på disse mails. Dette har også været en årsagerne til, at man har valgt at øge arbejdet med IT-sikkerhed yderligere. Man ønsker, at man i højere grad kan sortere disse mails fra og således minimere risikoen for at aktivere disse phishing-mails.

Virksomheden har valgt at samarbejde med eksterne partnere omkring enkelte elementer af deres IT-sikkerhed, da de vurderer, at de ikke har de nødvendige kompetencer til at håndtere alle tingene selv, hvorfor man ser det som essentielt for IT-sikkerheden at inddrage eksterne kompetencer. Således bliver brugen af eksterne partnere en måde at øge IT-sikkerheden på.

I og med virksomheden har valgt at få lavet en årlig ekstern analyse, er dette også med til at holde virksomheden skarp på IT-sikkerhed, da man ved, at man vil få testet dette igen, og man ønsker derfor at følge med, således denne test virker færrest mulige mangler.

Oplevede barrierer for at øge IT-sikkerhed

Hos Maskinhandler Indkøbsringen kan brugerne være en udfordring ift. IT-sikkerhed. For at implementere forskellige tiltag relateret til IT-sikkerhed, kræver det nogle gange, at man ændrer på arbejdsgange, -processer og –procedurer og det er medarbejderne ikke altid åbne over for. Medarbejderne ser det som besværligt og forstyrrende, og det kan være svært at se nødvendigheden i den skærpede sikkerhed. Man forsøger derfor hos Maskinhandler Indkøbsringen at implementere IT-sikkerhedstiltag, der påvirker medarbejderens daglige arbejde mindst muligt, således de ikke oplever nævneværdige ændringer.

Virksomheden oplever, at det er nødvendigt at finde en balance mellem økonomi og den nødvendige IT-sikkerhed. Maskinhandler Indkøbsringen ser, at de til tider er nødt til at fravælge IT-sikkerhedstiltag, fordi de ikke mener, at tiltagene er nødvendige, da virksomheden ikke vurderer, at de som virksomhed er særligt udsatte. Derfor behøver de ikke komplicerede tiltag. Man kan beskytte sig fuldstændigt, men det vil gøre det umuligt at arbejde og forstyrre driften, hvorfor det handler om at finde det IT-sikkerhedsniveau, der er nødvendigt.

Forventninger til fremtiden

Hos Maskinhandler Indkøbsringen oplever man ikke, at kunderne efterspørger eller spørger ind til IT-sikkerhed, og man forventer heller ikke, at dette vil ske i fremtiden. De ser dog, at de fortsat vil arbejde kontinuerligt med IT-sikkerhed og forsøge at følge med trusselsbilledet.

Virksomheden siger selv:

"Ledelsen betaler gladelig store summer penge for brandforsikringer og tyverisikringer, og det burde være det samme med IT-sikkerhed. Der er i princippet større risiko for, man bliver ramt på sin IT-sikkerhed."

7.4.9 **Case 9:** AB Hjem (anonymiseret virksomhed – navnet er et alias)

Om virksomheden

Navn | AB Hjem

Branche | Fast ejendom

Størrelse | 160 medarbejdere

Arketype | Tilpas sikker

AB Hjem er en udlejningsvirksomhed, der udlejer til private.

Virksomhedens IT-anvendelse

IT-sikkerhedsniveau| Middel

Risikoprofil | Middel

Virksomheden bruger IT til gængse ting som økonomistyring og personaledata og gemmer derudover data på de ejendomme, de udlejer. Derudover har AB Hjem et administrationssystem, hvor man administrerer udlejningen.

Introduktion til virksomhedens IT-sikkerhed

AB Hjem har implementeret diverse foranstaltninger for at øge deres IT-sikkerhed. Deres systemer ligger i et lukket netværk, og de er opmærksomme på, når en medarbejder fratræder at sikre, at denne medarbejder ikke længere har adgang til systemer eller data. Derudover har AB Hjem diverse produkter fra en ekstern IT-sikkerhedsleverandør, f.eks. firewalls, og bruger derudover en ekstern host til deres servere. Ligeledes tager AB Hjem backup af deres data hver dag, hvoraf de gemmer noget data i længere tid end andet. De tager flere backups, som lagres flere steder for at sikre, at de altid har en backup af deres systemer klar, hvis virksomheden skulle oplevere et IT-sikkerhedsbrud. Derudover har AB Hjem en klar procedure for, hvad de gør, såfremt de skulle opleve, at deres data eller systemer kompromitteres og har også forholdt sig til, hvordan de adresserer evt. ransomware. En gang årligt får de foretaget en sikkerhedsanalyse af en ekstern samarbejdspartner, som identificerer eventuelle huller, der skulle være i deres IT-sikkerhed.

AB Hjem har hidtil ikke haft meget fokus på IT-sikkerhed blandt medarbejderne, men vil arbejde mere med dette fremadrettet og vil i den forbindelse køre nogle interne træningsprogrammer.

AB Hjem har en IT-afdeling på ni medarbejdere, som løbende holder sig opdateret inden for IT. Derudover følger de med og forholder sig til, hvis de hører om et IT-sikkerhedsbrud i medierne og vurderer ud fra det, om virksomheden bør ændre i sin IT-sikkerhed.

Oplevede drivere for at øge IT-sikkerhed

AB Hjem fandt, at deres systemer var meget kritiske for deres forretning. AB Hjem så derfor, at de var nødt til at gøre en indsats på området. Hvis deres systemer går ned, har de mange medarbejdere, der ikke vil kunne arbejde, og de vil samtidig risikere at miste kunder. Således ser AB Hjem også en økonomisk driver for at øge deres IT-sikkerhed, da de både vil risikere at miste omsætning, men også have en alternativomkostning ved at have medarbejdere uden noget at lave.

En anden driver for AB Hjems forøgelse af IT-sikkerhed har været ledelsens øgede fokus på dette. Ledelsen har tidligere ikke været opmærksom på dette, men en større bevågenhed omkring dette fra mediernes side har været med til at øge ledelsens opmærksom på IT-sikkerhed og dermed også deres villighed til at afsætte flere ressourcer til området. Derudover bekræfter det også ledelsen i, at den indsats, der allerede er lagt, er den rette vej, og at man fortsat skal have fokus på området.

AB Hjems kunder er primært private kunder, men de har oplevet, at kunder har stillet spørgsmålstegn ved, at AB Hjems hjemmeside ikke var https, som betyder, at alle informationer og data sendes via en krypteret forbindelse. Dette har fået AB Hjem til at opdatere deres hjemmeside til https. Som kunde skal man derudover have en bruger, når man ønsker at betale, og her har kunder også bemærket, at adgangskoden ikke var skjult, når man skrev denne ind. Kunderne er således også en medvirkende faktor til, at AB Hjem har fokus på IT-sikkerhed, selvom dette er en mindre faktor ift. IT-sikkerhed.

Persondataforordningen har også været medvirkende til, at AB Hjem har arbejdet mere med IT-sikkerhed, da de er nødt til at følge med på dette område, og de oplever, at denne betyder, at AB Hjem også skal have mere fokus på IT-sikkerhed i fremtiden, og at den vil få betydning for hele organisationen.

Oplevede barrierer for at øge IT-sikkerhed

Inden AB Hjem påbegyndte deres indsats med IT-sikkerhed var en af de barrierer, de oplevede, manglende viden og fokus hos ledelsen. Ledelsen var på daværende tidspunkt ikke opmærksom på, hvad det kunne have af konsekvenser, hvis man kom ud for et IT-sikkerhedsbrud. Dette fik ledelsen dog en større forståelse for, da der kom mere fokus på IT-sikkerhed og IT-sikkerhedsbrud i medierne, og det blev mere klart, hvorfor IT-sikkerhed er vigtigt.

Derudover er medarbejderne en barriere for at øge IT-sikkerheden, da der på nuværende tidspunkt er meget lavt fokus på IT-sikkerhed blandt medarbejderne. Medarbejderne forholder sig ikke til IT-sikkerhed og tænker f.eks. ikke over, om deres password er stærkt nok. Hos AB Hjem ser man, at det kræver en kulturændring, hvor man i højere grad træner dette, f.eks. gennem awareness-træning.

Afsluttende ser AB Hjem, at det kan være problematisk at finde rundt i, hvad der er af tilbud og produkter på markedet og hvilke samarbejdspartnere, der er. AB Hjem bruger flere samarbejdspartnere på forskellige områder, og de oplever, at det kan være svært at vurdere, hvem der er de rette samarbejdspartnere for dem og ikke mindst, hvordan man identificerer disse. AB Hjem har endnu ikke fundet løsningen på denne barriere, men forsøger fortsat at navigere i de tilbud og produkter, der er.

Forventninger til fremtiden

AB Hjem har hidtil ikke brugt deres IT-sikkerhed i en kommerciel sammenhæng, men ser, at dette kan være en mulighed fremadrettet. AB Hjem ser en mulighed i at bruge dette i sin kommunikation mod kunderne, da det kan vise, at AB Hjem værner om deres oplysninger.

Virksomheden siger selv:

"Det er en jungle at finde ud af, hvad der er af produkter og muligheder på markedet, og hvem de rigtige samarbejdspartnere for os er."

7.4.10 **Case 10:** Sund og Bælt

Om virksomheden

Navn | Sund og Bælt

Branche | Transport og godshåndtering

Størrelse | 127 medarbejdere

Arketype | Påpasselig

Sund og Bælt er et holdingselskab, der ejer aktier i og har den overordnede styring af deres dattersel-skaber

Virksomhedens IT-anvendelse

IT-sikkerhedsniveau| Høj

Risikoprofil | Middel

Virksomheden opbevarer traditionel, administrativ data, herunder kundedata, som bl.a. indeholder kundernes brug af Storebæltsbroen. Herudover kortlægger virksomheden årligt de systemer, de har og har på baggrund af det identificeret en række systemer, som er kritiske for deres forretning.

Introduktion til virksomhedens IT-sikkerhed

Hos Sund og Bælt har man implementeret størstedelen af de grundlæggende IT-sikkerhedsforanstaltninger, som firewall og backup. Derudover får Sund og Bælt årligt udført en IT-revision, hvor en ekstern partner går deres IT-sikkerhed igennem og identificerer eventuelle huller. Sund og Bælt laver derudover en årlig intern risikovurdering, hvor de kortlægger alle systemer og spørger nøglepersoner i virksomheden, hvilke systemer, der er mest kritiske for dem, så de på den måde kan identificere de systemer, der er mest kritiske for virksomheden. På baggrund af risikovurderingen laver de en risikorapport og ud fra dette vurderer man, hvordan man håndterer de forskellige risici. Sund og Bælt bruger flere standarder fra 27000-serien (ISO-certificeringer), og de har ud fra disse standarder udvalgt det, der umiddelbart giver mening at bruge i virksomheden og lavet en række procedurer for, hvordan de arbejder med IT-sikkerhed. Ift. medarbejderne forsøger man hos Sund og Bælt at italesætte IT-sikkerhed og skabe en kultur, hvor det er i orden at stille spørgsmål og generelt tale om IT-sikkerhed. Det har man bl.a. gjort ved at italesætte, at det altid er i orden at komme ned til IT-afdelingen og stille spørgsmål vedr it-sikkerhed. Derudover søger de at gøre IT-sikkerhed håndgribeligt ved at bruge eksempler. Der er planlagt en awareness-kampagne internt i virksomheden for at sætte fokus på det blandt medarbejderne. Kampagnen er pt. planlagt til at løbe over de kommende 3 år.

Sund og Bælt har valgt ikke at outsource deres IT, men bruger eksterne leverandører på udvalgte områder, hvor deres egne kompetencer ikke er dækkende. Der er med andre ord tale om en form for multisourcing.

Hos Sund og Bælt får man i høj grad sin viden om IT-sikkerhed fra sine leverandører af IT-sikkerhedsprodukter og følger derudover med i, hvad der sker på området gennem abonnementer og via medierne.

Virksomheden har oplevet IT-sikkerhedsbrud og har også oplevet angreb, som deres systemer var i stand til at fange og stoppe, inden det fik konsekvenser for forretningen.

Oplevede drivere for at øge IT-sikkerhed

Hos Sund og Bælt ser man, at man i fremtiden kommer til at være mere data-drevet inden for flere af de områder virksomheden arbejder med i dag, og at IT generelt udvikler sig og bliver mere kompleks. I takt med denne udvikling ser Sund og Bælt også, at de er nødt til hele tiden at have IT-sikkerhed på dagsordenen. Det kræver, at man tænker det ind allerede i implementeringen af nye systemer, så det ikke er noget, man skal installere og bygge ovenpå efterfølgende. Denne tilgang er også et krav i forbindelse med Persondataforordningen der træder i kraft d. 25. maj 2018. Af forordningen fremgår det, at det er et krav at datasikkerhed (Privacy by Design, Privacy by Default) er tænkt ind i nye systemer, hvori der behandles persondata

Sund og Bælt er underlagt en årlig IT-revision. Revisionen hjælper til at holde fokus på de grundlæggende aspekter af it-sikkerheden.

Sund og Bælt har oplevet forsøg på angreb på deres IT-systemer. Det var muligt at stoppe dette angreb, men det bekræfter virksomheden i at IT-sikkerhed skal have høj attention. Persondataforordningen har betydet at Sund og

Bælt har brugt tid på at få afdækket, hvor man behandler persondata i virksomheden. Efterfølgende er Sund og Bælt gået i gang med at slette persondata, som ikke er kritiske for den daglige drift af virksomheden. Denne opgave er tidsmæssigt krævende og kræver tæt dialog med leverandører af it-systemerne, da mange systemer ikke er forberedt til at kunne slette data.

Oplevede barrierer for at øge IT-sikkerhed

Generelt oplever Sund og Bælt få barrierer i deres arbejde med IT-sikkerhed. De ser til tider, at medarbejderne kan stille sig uforstående over for, at forandringer er påkrævet, fordi medarbejderne føler at tingene fungerer, som de skal. Sund og Bælt har igangsat en awareness-kampagne, og har her valgt en leverandør, hvor et af kriterierne var at kommunikationen i høj grad skulle være målrettet medarbejderen således at budskaberne både kan anvendes i relation til det daglige arbejde i virksomheden, men også når man er på nettet privat. Derudover oplever Sund og Bælt til tider, at man kan være optimistisk i sin planlægning. Nogle af de mere komplekse tiltag på it-sikkerhedsområdet har skullet implementeres trinvist for ikke at påvirke den daglige arbejde for meget. Det giver et længere implementeringsforløb. Herudover har behovet for at opprioritere andre it-sikkerhedstiltag inden det foregående projekt var færdigimplementeret også betydet at tidshorisonten for nogle af projekterne er blevet forlænget.

Forventninger til fremtiden

Hos Sund og Bælt forventer man, at man i fremtiden kommer til at arbejde mere integreret med IT-sikkerhed, således at det bliver mere naturligt at tænke IT-sikkerhed ind, når man laver nye tiltag. Det bliver således ikke kun IT-afdelingen, der i fremtiden arbejder med it-sikkerhed, men i høj grad også de enkelte forretningsfunktioner i virksomheden.

7.4.11 **Case 11:** ToBu Transport (anonymiseret virksomhed – navnet er et alias)

Om virksomheden

Navn | ToBu Transport

Branche | Transport og godshåndtering

Størrelse | ~100 ansatte

Arketype | Påpasselig

ToBu Transport er et transportselskab, der primært henvender sig til private.

Virksomhedens IT-anvendelse

IT-sikkerhedsniveau | Høj

Risikoprofil | Middel

ToBu Transport bruger IT til gængse ting som økonomistyring og opbevaring af personaledata, men har ingen følsomme personoplysninger. Derudover har ToBu Transport systemer, der hjælper chaufførerne på deres ruter. ToBu Transport er en del af et fælles betalingsportal, men dette varetager ToBu Transport ikke selv.

Introduktion til virksomhedens IT-sikkerhed

ToBu Transport har implementeret en række grundlæggende og avancerede foranstaltninger, der øger deres IT-sikkerhed, herunder firewall, data protection software, scanningsfiltre, secure DNS og fysisk sikring af deres servere. Derudover har de specifikke administratorkontoer, således man skal være logget på en administratorkonto, hvis man skal ind og ændre på grundlæggende ting i IT-systemer. I IT-afdelingen har man også netop sendt en medarbejder på kursus om IT-sikkerhed for at øge den interne viden og kompetencer på området. IT-afdelingen har lavet et opgavehjul, hvor der kommer tilbagevendende påmindelser på opdateringer af IT-sikkerhed, som gør, at de kontinuerligt holder øje med deres IT-sikkerhed. Derudover får de årligt foretaget en sårbarhedsanalyse, som fortæller dem, hvordan deres IT-sikkerhedsniveau ser ud. I ToBu Transport oplyser man jævnligt medarbejderne om IT-sikkerhed og underviser i, hvordan man skal være opmærksom på mails o.lign. Man forsøger at arbejde kontinuerligt med det og forankre det i kulturen, således det er noget, man taler om og er opmærksom på.

ToBu Transport har udliciteret en stor del af deres IT, således de kun håndterer en mindre del internt, mens resten er lagt ud til en ekstern host. De har valgt at lægge en stor del IT-sikkerhed ud til en ekstern host, da de ikke har størrelsen til at have en ansat til at varetage dette. ToBu Transport ser også, at de på denne måde får adgang til flere kompetencer, end hvis de selv varetog al IT-sikkerhed.

Hos ToBu Transport har man ikke oplevet et IT-sikkerhedsbrud eller et forsøg herpå. Skulle deres systemer blive hackede, vil det være forstyrrende, men forretningen vil kunne fortsætte.

Virksomheden er med i to brancheforaer omkring IT-sikkerhed, hvor de kan dele viden og erfaringer med andre lignende virksomheder. Her har man også sammen kørt nogle IT-sikkerhedstests, og ToBu Transport oplever, at i disse fora får man både information om nye trusler samt kan dele erfaringer om nye tiltag.

Oplevede drivere for at øge IT-sikkerhed

ToBu Transport har arbejdet med at øge deres IT-sikkerhed for at være proaktive og forsøge at være foran. Virksomheden oplever, at de gennem deres eksterne host og nyhedsbreve generelt får meget information om, hvad der sker på markedet, og at de denne vej igennem kan holde sig opdaterede og træffe de nødvendige valg. Derudover er ToBu Transports deltagelse i IT-sikkerhedsfora også en driver for deres IT-sikkerhed, da det gør det muligt for dem at diskutere med ligesindede om, hvad der er relevant for dem og få indblik i andres erfaringer.

Ledelsen hos ToBu Transport har set positivt på IT-sikkerhed, og det, at ToBu Transport ikke har oplevet et IT-sikkerhedsbrud, giver genklang hos ledelsen og gør det nemmere at lave en fortsat indsats, fordi ledelsen kan se, at tiltagene virker. ToBu Transport bruger derudover deres IT-sikkerhed som kommunikation internt mod deres bestyrelse for at kunne redegøre for, at deres IT-sikkerhedsniveau er tilstrækkeligt.

En anden driver for ToBu Transport er, at de har en medarbejder, der tidligere har været i et forsyningsselskab, hvor IT-sikkerhed er meget essentielt. Han har derfor noget erfaring, som ToBu Transport har kunne bruge til at sætte ind på nye områder.

Oplevede barrierer for at øge IT-sikkerhed

ToBu Transport oplever få barrierer for at øge deres IT-sikkerhed. De ser dog, at den store informationsmængde, de modtager, kan gøre det svært at navigere i, hvad der er nødvendigt, og hvad der ikke er nødvendigt. Det kan være svært at trække essensen ud og vurdere, hvad der er relevant for dem.

Da ToBu Transport ikke oplever, at IT-sikkerhed er særligt kritisk for deres forretning opvejer de også hele tiden omkostningerne ved en foranstaltning mod effekten. De vurderer altid, hvad sandsynligheden for en given trussel er, og hvad det vil have af konsekvenser, og det betyder, at de til tider vurderer, at en foranstaltning vil være en overimplementering og unødvendig for deres virksomhed.

Forventninger til fremtiden

ToBu Transport forventer, at de i fremtiden vil arbejde med IT-sikkerhed på samme måde, som de gør i dag, hvor de kontinuerligt forholder sig til trusselsbilledet og deres eget sikkerhedsniveau. De forventer, at der vil ske en støt stigning i sikkerhedstrusler, men forventer, at de godt vil kunne følge med. Virksomheden ser dog, at der potentielt kan komme et større krav fra deres kunder om, at IT-sikkerheden er i orden, hvis der sker en stigning i IT-sikkerhed.

Virksomheden siger selv:

"IT-sikkerhedsbrud taler man mere om i dag, og det er ikke et tabu på samme måde som tidligere. Det er ikke på samme måde flovt, som det tidligere har været."

7.4.12 **Case 12:** TP Aerospace

Om virksomheden

Navn | TP Aerospace

Branche | Engroshandel og detailhandel

Størrelse | 220 medarbejdere

Arketype | Påpasselig

TP Aerospace sælger flyhjul og -bremser til mindre fly- og fragtselskaber og henvender sig til internationale markeder.

TP Aerospace har 7 lokationer rundt i verden.

Virksomhedens IT-brug

IT-sikkerhedsniveau | Middel

Risikoprofil | Lav

Virksomheden opbevarer personaledata, men intet der er direkte personfølsomt. Derudover har de et databasesystem med oversigt over varer.

Introduktion til virksomhedens IT-sikkerhed

TP Aerospace er på kort tid gået fra en meget lav grad af IT-sikkerhed til at arbejde målrettet med IT-sikkerhed, så de i dag har indført mange grundlæggende og avancerede tiltag som eksempelvis firewall, backup, IT-sikkerhedsprocedurer, og awareness-træning for medarbejderne. Derudover har TP Aerospace udliciteret deres server til en ekstern host, fordi man vurderer, at man ikke har kapaciteten til at varetage det internt. Man arbejder i IT-afdelingen målrettet med IT og har en projektplan for, hvad der skal implementeres hvornår og hvordan.

Man har hos TP Aerospace ikke oplevet et decideret IT-angreb, men har oplevet forsøg på phishing-mails. Skulle TP Aerospace systemer eller data blive ramt, vil det påvirke deres forretning, men de vil godt kunne fortsætte deres arbejde, da det primært er lageroplysninger omkring hvilke varer, virksomheden har på lager. Virksomheden har derudover en lang række certificeringer, som er nødvendige for deres arbejde, og hvis de mister disse certificeringer, vil de ikke kunne fortsætte deres forretning.

Hos TP Aerospace er deres primære kilde til viden gennem personlige netværk og derudover samarbejdspartnere, hvor de kan få viden om, hvad der sker på området, og hvad der er af nye produkter på markedet.

Oplevede drivere for at øge IT-sikkerhed

Den største driver for, at TP Aerospace har øget deres IT-sikkerhed har været, at de har opstartet en egentlig IT-funktion. Denne afdeling har haft fokus på at sikre virksomhedens IT-drift. Dette har indebåret en optimering af IT-sikkerheden. Virksomhedens IT-chef har brugt sin erfaring og viden fra tidligere stillinger til at bringe IT-sikkerheden op på et højere niveau som en del af sit arbejde med at opbygge en IT-afdeling, der kan sikre virksomhedens drift.

Derudover er der for TP Aerospace en driver i, at deres IT-chef vidensdeler og sparrer med andre personer inden for IT-branchen. Generelt forsøger den IT-ansvarlige at være i dialog med andre personer i sit netværk, der beskæftiger sig med IT–sikkerhed og ser det som en vigtig faktor i at finde ud af, hvad der er det rigtige for ens virksomhed ift. behov og omkostninger. IT-chefen har tidligere siddet i et formelt netværk med andre IT-chefer og ser, at det kunne være en mulighed at gå ind i et formelt netværk igen for i højere grad at sikre denne vidensdeling.

Hos TP Aerospace har ledelsen givet IT-afdelingen mandat til at implementere de nødvendige ting, og det har gjort det nemmere for IT-afdelingen at implementere de nødvendige foranstaltninger.

TP Aerospace har en række certificeringer, som de skal have for at kunne få lov at arbejde i den branche, de beskæftiger sig med. For at bevare disse certificeringer bliver virksomheden jævnligt udsat for auditeringer af, om de overholder de krav, der stilles til certificeringerne. Virksomheden oplever, at fordi de har styr på IT-sikkerheden, og de kan dokumentere dette, så går auditeringerne nemmere.

Oplevede barrierer for at øge IT-sikkerhed

Den primære barriere som TP Aerospace har oplevet i deres arbejde med IT-sikkerhed, har været medarbejdernes handlinger og begrænset viden om IT og IT-sikkerhed, hvilket bl.a. kom til udtryk ved, at medarbejderne ikke altid var indstillede på forandringerne, der kom som følge af, at man har øget IT-sikkerheden. For i højere grad at få medarbejderne med på disse forandringer, bruges der mere tid på at forberede medarbejderne på de forandringer, der kommer, og forklare hvad det er og ikke mindst, hvorfor det er nødvendigt. Det er en igangværende ændring af kulturen for at skabe en større forståelse omkring IT-sikkerhed og således skabe en mere bevidst tilgang til IT. Dette består bl.a. i, at der deles viden gennem et nyhedsbrev og en blog.

I visse tilfælde har TP Aerospace været nødsaget til at udskyde enkelte tiltag, fordi de har måtte omprioritere. Da der er tale om en lille IT-afdeling, er der en naturlig ressourcebegrænsning, som gør, at TP Aerospace oplever, at de nogle gange kan være nødsaget til at vente med at implementere et tiltag.

Forventninger til fremtiden

TP Aerospace er stadig i gang med deres indsats med at øge IT-sikkerheden og har derfor allerede planer om at øge sikkerheden og implementere flere tiltag på området. De vil fortsat følge med i udviklingen på området og så vidt muligt handle proaktivt på området.

Virksomheden siger selv:

"Det er en jungle, så man er nødt til at erfaringsdele og sparre med andre for at finde ud af, hvad der passer bedst til ens virksomhed."

7.4.13 **Case 13:** Blå Maritim (anonymiseret virksomhed – navnet er et alias)

Om virksomheden

Navn | Blå Maritim

Branche | Transport og godshåndtering

Størrelse | 100 medarbejdere

Arketype | Påpasselig

Virksomheden er en maritim virksomhed, der beskæftiger sig inden for transportbranchen.

Virksomhedens IT-anvendelse

It-sikkerhedsniveau | Middel

Risikoprofil | Lav

Virksomheden opbevarer medarbejderdata, men intet der er personfølsomt. Derudover opbevarer de data omkring deres kunder. Virksomheden har økonomisystem og et system til dokumenthåndtering, men det er ikke systemer, der er forretningskritiske

Introduktion til virksomhedens IT-sikkerhed

Blå Maritim har udliciteret størstedelen af deres IT, og det er derfor deres leverandører, der er den primære kilde til IT-sikkerhed. Leverandørerne skal underskrive en kontrakt omkring IT-sikkerhed, hvor Blå Maritim stiller nogle krav til, hvordan dette håndteres, fordi Blå Maritim ønsker, at disse leverandører har fokus på IT-sikkerhed.

Derudover har man internt i virksomheden fokus på IT-sikkerhed. Man har kørt en awareness-kampagne målrettet mod medarbejderne, og man forventer også at køre dette igen på et senere tidspunkt. Derudover har man forskellige arbejdsgrupper i virksomheden, hvoraf en specifikt handler om IT-sikkerhed.

Hos Blå Maritim får man primært sin viden om IT-sikkerhed fra de leverandører, man bruger, som jævnligt kommer i huset.

Oplevede drivere for at øge IT-sikkerhed

Den primære driver for Blå Maritims arbejde med sikkerhed er for at sikre driftssikkerheden. Man ønsker at sikre, at IT-systemer fungerer, og data kan tilgås uden forstyrrelser og nedbrud. Dette hænger også tæt sammen med det image, man ønsker at bevare over for sine kunder. Man ønsker at sikre, at kunderne opfatter en som professionel både driftsmæssigt og i håndtering af kunders data. En anden driver for arbejdet med IT-sikkerhed i Blå Maritim er bl.a., når man oftere og oftere ser tilfælde af IT-sikkerhedsbrud hos andre virksomheder i medierne. Dette øger opmærksomheden, og virksomheden nævner, at de ser IT-sikkerhed som noget, man løbende skal vedligeholde.

Man har hos Blå Maritim oplevet et IT-sikkerhedsbrud i form af ransomware. IT-sikkerhedsbruddet ramte heldigvis kun en enkelt computer, fordi virksomheden fik lukket ned for det, før det spredte sig. Dette var en medvirkende faktor til, at man iværksatte awareness-kampagner for at øge opmærksomheden og bevidstheden omkring IT-sikkerhed og potentielle trusler.

Man oplever hos Blå Maritim, at man har opnået en højere IT-sikkerhed ved at udlicitere størstedelen af sin IT. De har ikke de nødvendige kompetencer internt, og derfor gør brugen af eksterne leverandører, at de opnår en højere grad af IT-sikkerhed.

Oplevede barrierer for at øge IT-sikkerhed

Medarbejdernes manglende viden om og forståelse for IT-sikkerhed er den primære barriere for at øge IT-sikkerheden i Blå Maritim. Medarbejderne har mange forskellige baggrunde og uddannelser, og man oplever, at det kan gøre kommunikationen svær, da den skal målrettes de forskellige grupper af medarbejdere. Det er meget forskelligt, hvad de forskellige medarbejdere har brug for af information, fordi de løser mange forskellige opgaver og derfor bruger IT i forskellig grad. Man har hos Blå Maritim imødekommet dette ved at have generelle awareness-kampagner, og derudover tilpasse kommunikationen, således man inddrager den enkelte afdelingsleder, og i nogle

tilfælde i højere grad inddrager IT-afdelingen i kommunikationen. Virksomheden oplever, at medarbejderne godt forstår, hvorfor IT-sikkerhed er vigtigt, men at de finder det besværligt, f.eks. når de skal ændre deres adgangskoder.

Derudover er den almindelige prioritering af arbejdsopgaver til tider også en barriere, der gør, at man er nødt til at udskyde en opgave, fordi man ikke har den nødvendige tid til rådighed.

Forventninger til fremtiden

Blå Maritim forventer, at de vil fortsætte arbejdet med IT-sikkerhed i fremtiden, og at det potentielt vil kræve flere ressourcer. De vil søge at være på forkant, men anerkender også, at det er meget svært, og man kan risikere at blive ramt. På nuværende tidspunkt bruger Blå Maritim det ikke i sin kommunikation til kunderne, men det vil potentielt være noget, de vil gøre i fremtiden.

Virksomheden siger selv:

"Vi har mange forskellige typer af medarbejdere, og der er stor forskel på, hvad de har brug for af information om IT-sikkerhed. Vi prøver derfor at inddrage afdelingsFremtidens Læring udover den generelle information om IT-sikkerhed."

7.4.14 **Case 14:** Aarhus Teater

Om virksomheden

Navn | Aarhus Teater

Branche | Kultur, forlystelser og sport

Størrelse | 100-249 medarbejdere

Arketype | Tilpas sikker

Aarhus Teater laver teaterforestillinger

Virksomhedens IT-anvendelse

IT-sikkerhedsniveau | Middel

Risikoprofil | Middel

Virksomheden lagrer data vedr. forestillinger, som indeholder alle detaljer omkring en forestilling. Derudover oplysninger omkring skuespillerne, kommende teaterprogrammer og manuskripter. Derudover har man et billetsystem, der er kritisk for forretningen, da det er her igennem, omsætning genereres. Derudover har man økonomisystem og HR-system, som opbevarer mindre kritiske data.

Introduktion til virksomhedens IT-sikkerhed

Hos Aarhus Teater har man tidligere brugt enkelte IT-systemer af ældre dato, og man er i gang med at opdatere sine IT-systemer og herunder øge IT-sikkerheden. Virksomheden har valgt at outsource en stor del af deres IT, herunder virksomhedens servere, da man ikke ser, at man har tilstrækkelige ressourcer eller intern viden til at løfte opgaven. Man har implementeret en række tiltag ift. IT-sikkerhed, bl.a. backup, 6 lag sikkerhed på mails, filtrering på hjemmesider, lukkede netværk, regler omkring brug af USB, IT-sikkerhedspolitik, awareness-træning af medarbejdere samt løbende intern kommunikation, og man har derudover afskåret forestillinger fra IT, således en forestilling aldrig vil blive påvirket af IT-sikkerhedsbrud, mens den er i gang.

Virksomheden har oplevet et IT-sikkerhedsbrud, hvor knap 11.000 af deres 300.000 filer blev krypterede, inden de lokaliserede kilden og fik stoppet IT-sikkerhedsangrebet. Kilden var en mail med et link, som en medarbejder var kommet til at trykke på. Det omfattende IT-sikkerhedsbrud fik man løst i samarbejde med virksomhedens partnere, men virksomheden kunne ikke bruge IT i knap fire dage.

Hos Aarhus Teater får man viden omkring IT-sikkerhed gennem sine leverandører og ved selv at opsøge viden. Derudover er den IT-ansvarlige medlem af NC3 Skyt, hvorigennem virksomheden også får meget viden og opdateringer omkring IT-sikkerhed.

Oplevede drivere for at øge IT-sikkerhed

Man oplever hos Aarhus Teater, at det giver en større IT-sikkerhed, at man har valgt at outsource en stor del af IT, da man på denne måde får adgang til flere kompetencer, end man kan have internt, og derudover nogle, som kun beskæftiger sig med dette.

Det at Aarhus Teater har været udsat for et IT-sikkerhedsbrud, som påvirkede deres forretning, har været en stor driver for deres videre arbejde med IT-sikkerhed. Bruddet betød, at man blev mere opmærksom på de IT-sikkerhedsforanstaltninger, man havde implementeret, og det skabte derudover et større fokus på IT-sikkerhed i virksomheden. Risikoen blev meget klar, hvilket gjorde det mere håndgribeligt for medarbejderne at forholde sig til IT-sikkerhed.

Derudover ønsker man at være proaktiv hos Aarhus Teater og hele tiden følge med det IT-trusselsbillede, der ændrer sig. For at sikre driften er man nødt til at følge med og holde sig opdateret, både på viden, men også de foranstaltninger, det kræver.

Oplevede barrierer for at øge IT-sikkerhed

Aarhus Teater er en virksomhed med mange kreative mennesker, som ikke nødvendigvis har daglig berøring med og stor viden om IT og IT-sikkerhed. Derfor ligger der en vigtig kommunikationsopgave i at skabe den fornødne opmærksomhed om og forståelse for IT-sikkerhed på arbejdspladsen. Udover jævnligt at komme rundt i de forskel-

lige afdelinger, arbejder man med små videokurser og informerende mails. Herudover har man valgt, at medarbejderne fremover ikke skal have adgang til alle drev, men kun dem, der har særlig relevans for dermed at reducere fejlrisiciene. Teatrets ledelse ser brugerne som den vigtigste del af IT-sikkerheden, og det er afgørende, at personalet har den fornødne viden og forståels, for hvis noget slipper igennem de tekniske foranstaltninger, så er medarbejderne det sidste forsvar.

Derudover handler det for Aarhus Teater om at finde den nødvendige balance for, hvor sikret man skal være, og hvor mange ressourcer man skal bruge på IT-sikkerhed. Man kan ikke nå den perfekte IT-sikkerhed, og man skal derfor finde det niveau, der passer til virksomheden. Derudover handler IT-sikkerhed om prioritering i en travl hverdag, hvor man med teaterproduktion har mange deadline-afhængige opgaver, hvilket kan betyde, at man kan være nødt til at udskyde visse IT-sikkerhedsrelaterede opgaver.

Forventninger til fremtiden

Virksomheden har oplevet, at medarbejderne selv er begyndt at tænke over IT-sikkerhed og komme med forslag til nye tiltag, herunder hvordan man sikkert kan streame optagelser af en forestillingsprøve, når man har en person, der sidder et andet sted i landet. Man ser dette som en positiv udvikling og håber, at medarbejderne også fremadrettet vil engagere sig i IT-sikkerhed.

Virksomheden siger selv:

"Hvis alle medarbejdere klædes tilstrækkeligt på til at forstå vigtigheden af IT-sikkerhed og konsekvenserne i dagligdagen ved et angreb, behøver man næsten ikke andre tiltag mod phishingmails."

Monitor
Deloitte.

Om Deloitte
Deloitte leverer ydelser indenfor revision, consulting, financial advisory, risikostyring, skat og dertil knyttede ydelser til både offentlige og private kunder i en lang række brancher. Deloitte betjener fire ud af fem virksomheder på listen over verdens største selskaber, Fortune Global 500®, gennem et globalt forbundet netværk af medlemsfirmaer i over 150 lande, der leverer kompetencer og viden i verdensklasse og service af høj kvalitet til at håndtere kundernes mest komplekse forretningsmæssige udfordringer. Vil du vide mere om, hvordan Deloittes omkring 245.000 medarbejdere gør en forskel, der betyder noget, så besøg os på Facebook, LinkedIn eller Twitter.