Monitor Deloitte

IT-sikkerhed i danske SMV'er – et sammendrag

Monitor Deloitte for Erhvervsstyrelsen

April 2018

Kort om undersøgelsen

Monitor Deloitte har for Erhvervsstyrelsen undersøgt IT-sikkerhedsniveauet i små og mellemstore virksomheder (SMV'er) i Danmark. Analysen er lavet på basis af en telefonisk spørgeskemaundersøgelse af 1.054 danske virksomheder samt kvalitative interview med 14 udvalgte SMV'er. Analysen er gennemført i efteråret 2017.

Denne publikation er et sammendrag af den fuldstændige rapport: "IT-sikkerhed og datahåndtering i danske SMV'er", som kan hentes på Erhvervsstyrelsens hjemmeside.

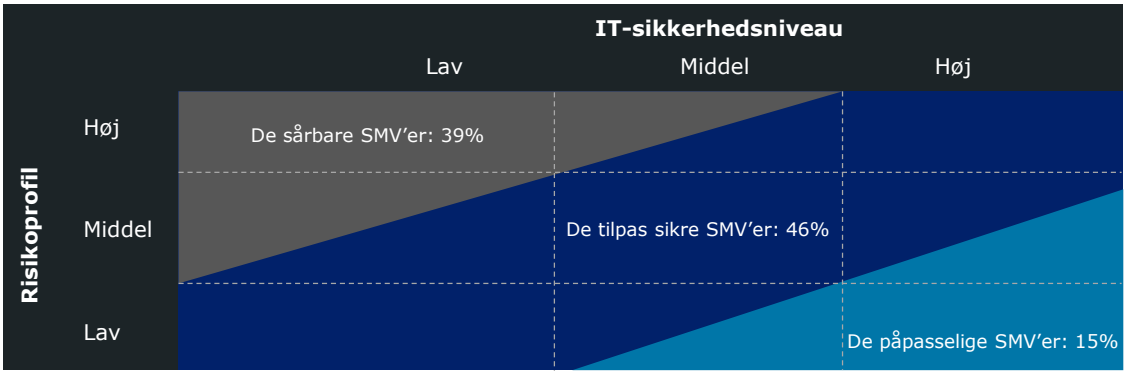
Undersøgelsens nøgleresultater

- 39 procent af danske SMV'er har ikke den rette balance mellem risikoprofil og IT-sikkerhedsniveau, hvilket øger deres sårbarhed overfor IT-sikkerhedsangreb.
- Knap en fjerdedel af danske SMV'er har ikke implementeret de mest essentielle IT-sikkerhedsforanstaltninger, herunder systematisk backup.
- Ledelsens viden om og fokus på IT-sikkerhed har stor betydning for IT-sikkerhedsniveauet i de danske SMV'er. Det samme gælder for medarbejdere, herunder IT-ansvarlige.
- For 16 procent af danske SMV'er kan konsekvensen ved et læk af forretningskritiske data være, at de mister deres forretningsgrundlag.

39 PROCENT AF DANSKE SMV'ER ER SÆRLIGT SÅRBARE OVERFOR IT-SIKKERHEDSANGREB

På baggrund af besvarelserne fra spørgeskemaundersøgelsen sammenstilles SMV'ernes tiltag og foranstaltninger med virksomhedernes risikoprofil, og her er konklusionen desværre, at en stor del af de danske SMV'er ikke har et tilstrækkeligt IT-sikkerhedsniveau og derfor er særligt sårbare overfor IT-sikkerhedsangreb.

Figur 1. SMV'ernes IT-sikkerhedsniveau i forhold til risikoprofil



Note: Figuren viser SMV'ers vægtede fordeling indenfor arketyperne, det vil sige sammenhæng mellem virksomhedernes IT-sikkerhedsniveau og risikoprofil.

Kilde: Wilke for Monitor Deloitte og Monitor Deloitte-analyse.

Virksomheder bør have balance mellem deres risikoprofil og IT-sikkerhedsniveau, så de har implementeret et tilstrækkeligt IT-sikkerhedsniveau i forhold til deres risikoprofil. I Figur 1 holdes virksomhedernes risikoprofil op imod virksomhedernes IT-sikkerhedsniveau, og her fremgår det, at 39 procent af de danske SMV'er ikke har en tilstrækkelig balance mellem deres IT-sikkerhedsniveau og deres risikoprofil. Dette øger virksomhedernes sårbarhed overfor IT-sikkerhedsbrud, hvilket kan være kritisk for virksomhederne.

Risikoprofilen vurderes på baggrund af virksomhedens anvendelse af IT-systemer, opbevaring af følsomme data samt branche. IT-sikkerhedsniveauet evalueres på baggrund af tre forskellige faktorer relateret til virksomhedens generelle IT-sikkerhed: medarbejdere og ledelse, IT-sikkerhedsforanstaltninger samt fysisk adgangskontrol. Virksomhederne i de forskellige grupper har forskellige karakteristika.

Over halvdelen af danske SMV'er vurderes at have et lavt IT-sikkerhedsniveau, hvilket blandt andet skyldes, at mange ikke har implementeret essentielle IT-sikkerhedsforanstaltninger, der dækker systematiske og løbende opdateringer af systemer samt dokumenteret og gennemtestet backupprocedurer.

Denne undersøgelse viser, at ledelsens stillingtagen til IT-sikkerhed har stor betydning for virksomhedernes IT-sikkerhedsniveau: I jo højere grad, ledelsen har taget stilling til IT-sikkerhed, des højere er virksomhedens IT-sikkerhedsniveau. Ledelsens stillingtagen er tæt relateret til dens viden om IT-sikkerhed, og det er derfor vigtigt, at ledelsen har tilstrækkelig viden om IT-sikkerhed. Dette gælder også for medarbejderne, så de bedst muligt kan bidrage til virksomhedens IT-sikkerhed. I særdeleshed er det centralt, at den IT-ansvarlige har et tilstrækkeligt videnniveau om IT-sikkerhed, så han/hun er i stand til at vurdere, hvordan virksomhedens IT-sikkerhedsniveau bør være.

Utilstrækkelig IT-sikkerhed øger sårbarheden overfor IT-sikkerhedsbrud, og konsekvenserne af et sådant brud kan være omfattende for en virksomhed. Konsekvenserne kan dække omkostninger til at genetablere IT-systemer og data eller betaling af en løsesum for at få låst krypteret data op. Det kan også få mere langvarige konsekvenser på den måde, at virksomheden mister omsætning eller kunder, fordi deres image forringes. 16 procent af danske SMV'er svarer, at en læk af forretningskritiske data i yderste konsekvens kan betyde, at virksomheden mister sit forretningsgrundlag.

De påpasselige SMV'er er virksomheder med en lav grad af følsomme data. Blot 28 procent af virksomhederne i dette segment svarer, at deres systemer behandler forretningskritiske data. Omvendt har alle virksomhederne sikret grundlæggende foranstaltninger og flere avancerede tiltag.

De tilpas sikre SMV'er er virksomheder med varierende anvendelse af data og systemer. Et kendetegn ved virksomhederne i denne kategori er, at de har et IT-sikkerhedsniveau, der er tilpasset deres risikoprofil.

De sårbare SMV'er er virksomheder med afhængighed af systemer i den daglige drift og afhængighed af flere typer følsomme data. På trods af dette har mange af virksomhederne ikke styr på grundlæggende IT-sikkerhedsforanstaltninger. Ledelsesinvolveringen er ligeledes lav for disse virksomheder.

DANSKE SMV'ER SKAL SE DERES IT-SIKKERHEDSNIVEAU I RELATION TIL DERES IT-ANVENDELSE OG RISIKOPROFIL

IT-sikkerhed skal ses i relation til den kontekst, den enkelte virksomhed opererer i. Ofte kan virksomhedernes vækst- og værdiskabende digitale løsninger være en medvirkende årsag til, at der opstår IT-sikkerhedsrelaterede risici. Dette skyldes, at de digitale løsninger er afhængige af systemer eller består af kritiske informationer, som konkurrenter eller kriminelle ikke må komme i besiddelse af eller påvirke driften af. Som denne undersøgelse viser, har mange danske SMV'er ikke et tilstrækkeligt fokus på deres IT-sikkerhed, til trods for at virksomhederne er dybt afhængige af IT-systemer og opererer med følsomme data.

Danske SMV'er bør derfor gøre mere for at sikre et tilstrækkeligt og gennemtænkt IT-sikkerhedsniveau ved at tilpasse indsatsen til virksomhedens IT-anvendelse og risikoprofil. Når en virksomhed skal afgøre sin risikoprofil skal der tages højde for tre elementer, ligesom en virksomheds IT-sikkerhedsniveau består af tre elementer, som det fremgår af nedenstående figur.

På de følgende sider gennemgås både risikoprofil og IT-sikkerhedsniveau mere detaljeret.

Figur 2. Faktorer, som tilsammen udgør risikoprofilen og IT-sikkerhedsniveauet

Kilde: Monitor Deloitte

På tværs af det danske SMV-segment er der en høj afhængighed af IT-systemer. 95 procent af de danske SMV'er er afhængige af IT-systemer i forhold til deres drift.

Kilde: IT-sikkerhed og datahåndtering i danske SMV'er

For at kunne vurdere, om en virksomheds IT-sikkerhedsniveau er tilstrækkeligt, bør vurderingen tage virksomhedens risikoprofil i betragtning.

Kilde: IT-sikkerhed og datahåndtering i danske SMV'er

RISIKOPROFIL – HVORDAN FASTSÆTTES DEN?

Det er vigtigt at kende til virksomhedens risikoprofil, da indsatserne relateret til IT-sikkerhed skal tilpasses derefter. Risikoprofilen giver et kontekstuelt billede af virksomhedens IT-trusselsbillede, det vil sige, hvor omfattende et IT-sikkerhedsbrud kunne blive for virksomheden samt sandsynligheden for et IT-sikkerhedsangreb. Risikoprofilen er et godt sted for virksomheder at starte, fordi den er relevant for de initiativer, virksomheden skal igangsætte. Risikoprofilen skal ses i sammenhæng med virksomhedens IT-sikkerhedsniveau for at begrænse risikoen for sårbarhed overfor IT-sikkerhedsangreb.

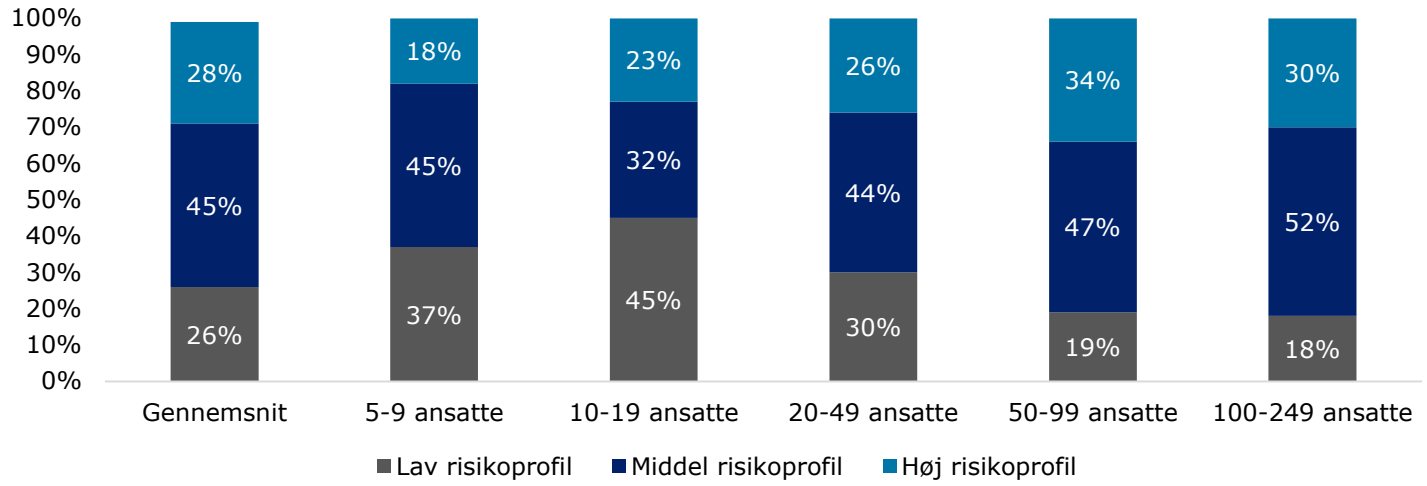
Hvis virksomheden opbevarer en stor mængde fortrolige, forretningskritiske data, er det vigtigt, at virksomheden har fokus på IT-sikkerhed. Omvendt er det vigtigt, at virksomheden ikke overimplementerer i forhold til sin risikoprofil, da dette kan medføre spildte ressourcer for virksomheden.

Risikoprofilen er grundlæggende afhængig af fire parametre:

1. I hvilken grad virksomheden er afhængig af IT-systemer i forhold til virksomhedens daglige drift.
2. I hvilken grad virksomheden gemmer følsomme personoplysninger såsom informationer om personers køn, seksualitet, politiske overbevisning, etnicitet, mv.
3. I hvilken grad virksomheden gemmer forretningskritiske data, herunder patentansøgninger, intellektuelle rettigheder, følsomme persondata og forretningshemmeligheder.
4. Branchen, som virksomheden opererer i (finanssektoren er eksempelvis traditionelt mere udsat end andre brancher).

Risikoprofilen er vurderet for alle 1.054 virksomheder, der deltog i spørgeskemaundersøgelsen på baggrund af ovenstående parametre. Overordnet set har 26 procent af danske SMV'er en lav risikoprofil, 45 procent har en middel risikoprofil, mens 28 procent har en høj risikoprofil (grundet afrundingen stemmer dette ikke til 100 procent). Derudover ses der en tendens til, at større virksomheder har en højere risikoprofil end mindre virksomheder, som det fremgår af nedenstående.

Figur 3. Gennemsnitlig risikoprofil samt fordeling på virksomhedsstørrelse



Kilde: Wilke for Monitor Deloitte og Monitor Deloitte-analyse

60 procent af de danske SMV'er gemmer følsomme personoplysninger. 44 procent gemmer forretningskritiske data.

Kilde: IT-sikkerhed og datahåndtering i danske SMV'er

Af de virksomheder, der gemmer forretningskritiske data, svarer 36 procent, at en læk af forretningskritiske data vil betyde, at de mister deres forretningsgrundlag. Dette svarer til 16 procent af hele populationen.

Kilde: IT-sikkerhed og datahåndtering i danske SMV'er

RISIKOVURDERINGER OG IT-SIKKERHEDSSTANDARDER SOM GRUNDLAG FOR ARBEJDET MED IT-SIKKERHED HOS SUND & BÆLT

Om virksomheden

Navn | Sund & Bælt

Branche | Transport og godshåndtering

Størrelse | 127 medarbejdere

Sund & Bælt er et holdingselskab, der ejer aktier i og har den overordnede styring af deres datterselskaber: A/S Storebælt, Sund & Bælt Partner A/S, Brobizz A/S, A/S Femern Landanlæg og Femern A/S.

Virksomhedens IT-anvendelse

Virksomheden opbevarer traditionelle, administrative data, herunder kundedata, som blandt andet indeholder kundernes brug af Storebæltsbroen.

Herudover kortlægger virksomheden årligt de systemer, de har, og har på baggrund heraf identificeret en række tekniske systemer, som er kritiske for deres forretning.

Sund & Bælt er ansvarlig for at drive kritisk infrastruktur og har en ejerstruktur og eksterne interessenter, der har klare forventninger til, at virksomheden har et tilstrækkeligt IT-sikkerhedsniveau og håndterer data på en ordentlig måde. Virksomhedens ønske om at leve op til denne tillid har været en væsentlig driver for arbejdet med IT-sikkerhed i virksomheden. Hos Sund & Bælt ser man, at man i fremtiden kommer til at være mere data-drevet indenfor 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 & 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.

Virksomheden har derfor valgt at implementere en meget struktureret og koordineret tilgang til IT-sikkerhed. Sund & 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 udarbejdet en række procedurer for, hvordan de arbejder med IT-sikkerhed. Standarderne fungerer derfor nærmest som en huskeliste for Sund & Bælt. Udfordringen med denne tilgang har været, at brugen af ISO-standarder kræver, at man tilpasser dem og de bagvedliggende processer og aktiviteter til virksomheden, hvilket kræver ressourcer og modenhed. Det er vigtigt at have for øje, at IT-sikkerheden passer til virksomheden og virksomhedskulturen.

Sund & Bælt foretager en årlig, intern risikovurdering, hvor de kortlægger alle systemer og spørger nøglepersoner i virksomheden, hvilke systemer der er mest kritiske for dem, for på den måde at identificere de systemer, der er mest kritiske for virksomheden. På baggrund af risikovurderingen udarbejder de en risikorapport, og ud fra dette vurderer man, hvordan man håndterer de forskellige risici. Virksomheden har særskilt vurderet, hvilken indflydelse IT-sikkerhedsangreb på specifikke systemer vil have på medarbejdernes mulighed for at arbejde, hvilket vil være kritisk for driften, og bruger denne analyse til at fastlægge deres IT-sikkerhedsniveau, så der gøres mest muligt for at undgå tab af arbejdstid som følge af IT-sikkerhedsangreb.

Selvom arbejdet er særdeles struktureret og baseret på ISO-standarder, vurderer IT-ledelsen, at det er en overkommelig opgave, netop fordi standarderne er med til at gøre det lettere at lave en pragmatisk vurdering af risici og tiltag, som er til at have med at gøre, og som kan kommunikeres til organisationens medarbejdere.

*ISO refererer til en anerkendt IT-sikkerhedsstandard, fx ISO27001 eller ISO27032.

> *Der er en masse standarder, man kan læne sig op ad, og man kan let opbygge et system, der er forholdsvis pragmatisk.*

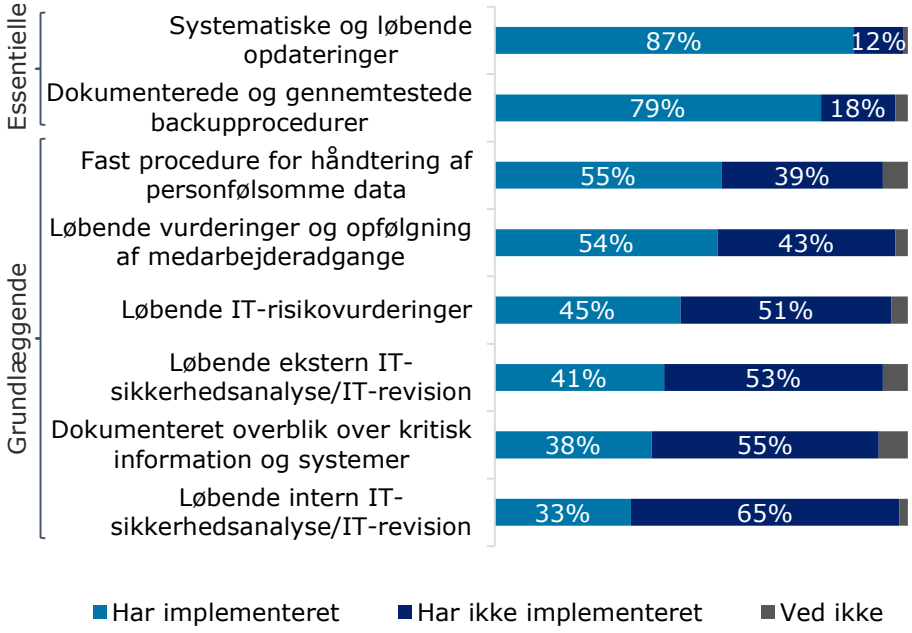
Sund & Bælts egen refleksion, på baggrund af deres oplevelser med IT-sikkerhed

IT-SIKKERHEDSNIVEAUET: MANGE DANSKE SMV'ER HAR IKKE IMPLEMENTERET ESSENTIELLE TILTAG

Når man skal vurdere en virksomheds IT-sikkerhedsniveau, er tre elementer særligt relevante: medarbejdere og ledelse, IT-sikkerhedsforanstaltninger og fysisk adgangskontrol.

I forbindelse med IT-sikkerhedsforanstaltninger er der nogle essentielle og grundlæggende IT-sikkerhedsforanstaltninger, som langt de fleste virksomheder bør implementere. Undersøgelsen peger på, at 12 procent af danske SMV'er ikke har implementeret systematiske og løbende opdateringer, som er helt centralt i forhold til at lukke systemhuller for IT-kriminelle. Derudover har 18 procent ikke dokumenterede og gennemtestede backupprocedurer. Disse to IT-sikkerhedsforanstaltninger anses for helt essentielle for en virksomheds IT-sikkerhed. Ser man på de to faktorer samlet, har 23 procent, det vil sige knap en fjerdedel, af danske SMV'er ikke begge disse essentielle IT-sikkerhedsforanstaltninger som en del af deres IT-sikkerhed.

Figur 4. Essentielle og grundlæggende IT-sikkerhedsforanstaltninger



Note: Figuren viser den vægtede andel af SMV'er, der har implementeret essentielle og grundlæggende IT-sikkerhedsforanstaltninger.
Kilde: Wilke for Monitor Deloitte.

Med så stor en andel af danske SMV'er, der ikke har styr på disse centrale tiltag, vil mange SMV'er være meget sårbare i tilfælde af et IT-sikkerhedsbrud, som kan have store konsekvenser for en virksomhed.

Der er også en stor del af virksomhederne, der ikke har implementeret andre grundlæggende IT-sikkerhedstiltag. 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-sikkerheds-analyse og/eller IT-revision).

Undersøgelsens resultater peger på, at mange virksomheder ikke har overblik over, hvilke risici de står overfor, og/eller iværksætter grundlæggende foranstaltninger for at undgå eller afbøde virkningerne af et IT-sikkerhedsangreb.

Medarbejdere og ledelse

Medarbejdere og ledelse dækker ledelsens stillingtagen til IT-sikkerhed, træning af medarbejdere samt kommunikation til medarbejdere.

IT-sikkerhedsforanstaltninger

IT-sikkerhedsforanstaltninger er de tekniske, organisatoriske og processuelle foranstaltninger, som virksomheden har implementeret. Disse tiltag kan deles op i essentielle, grundlæggende og avancerede IT-sikkerhedsforanstaltninger.

Fysisk adgangskontrol

Fysisk adgangskontrol har at gøre med, i hvilken grad virksomheden styrer den fysiske adgang til henholdsvis kontoret og virksomhedens server.

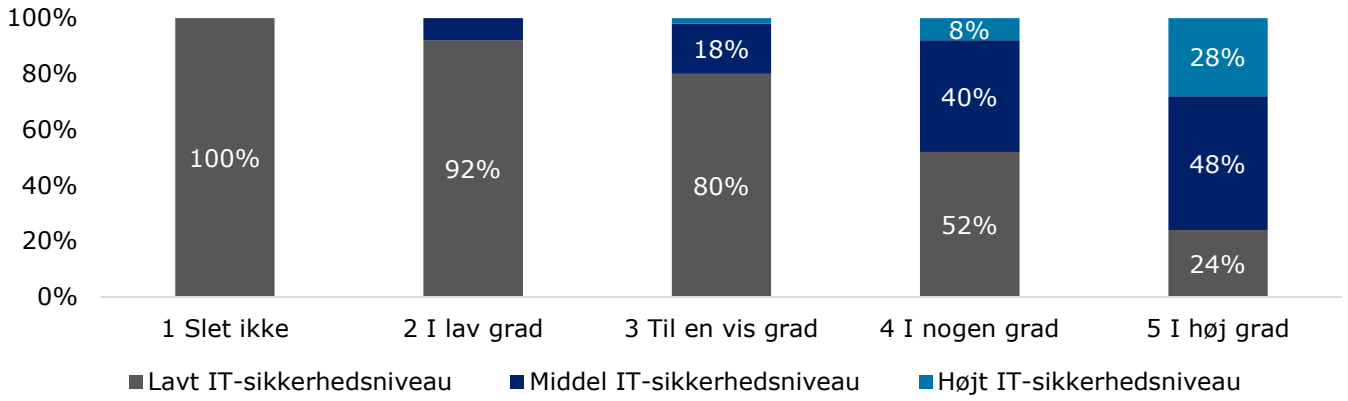
IT-SIKKERHED ØGES, NÅR VIRKSOMHEDENS LEDELSE HAR TAGET STILLING

I mange virksomheder er IT-sikkerhed forankret hos den IT-ansvarlige. Undersøgelsen viser dog, at det er afgørende for virksomhedens IT-sikkerhed, at ledelsen engagerer sig. Virksomhederne oplever dog, at ledelsen ikke altid engagerer sig i IT-sikkerhed, hvilket udgør en central barriere for arbejdet med dette. En måde at øge virksomhedernes IT-sikkerhed på er derfor at engagere ledelsen mere ved at give dem mere viden om IT-sikkerhed.

Ledelsesfokus kan øge IT-sikkerhedsniveauet

Flere af casevirksomhederne påpeger ledelsens manglende engagement i IT-sikkerhed som en barriere for IT-sikkerheden i virksomheden. Årsagen hertil er todelt: dels allokerer ledelsen ikke tilstrækkelige ressourcer til virksomhedens IT-sikkerhed, dels har ledelsens manglende engagement en afsmittende effekt på virksomhedskulturen og dermed medarbejderne.

Figur 5. Ledelsens stillingtagen til IT-sikkerhed og IT-sikkerhedsniveauet



Note: Tallene er vægtede.
Kilde: Wilke for Monitor Deloitte og Monitor Deloitte-analyse.

Som det ses af Figur 5, er der en tæt sammenhæng mellem ledelsens stillingtagen til IT-sikkerhed og virksomhedens IT-sikkerhedsniveau. I takt med at ledelsen i højere grad har taget stilling til IT-sikkerheden, stiger virksomhedernes IT-sikkerhedsniveau. Dette indikerer, at ledelsens stillingtagen også kan være en drivkraft for at øge IT-sikkerhedsniveauet.

For at øge ledelsens forståelse og er flere IT-ansvarlige i virksomhederne begyndt i højere grad at informere ledelsen om IT-sikkerhed og eventuelle konsekvenser ved manglende IT-sikkerhed. Den mundtlige kommunikation kan bidrage til at øge ledelsens fokus ved kontinuerligt at skubbe information til ledelsen. Udover den mundtlige kommunikation peger flere af virksomhederne også på, at det er værdifuldt at få udarbejdet en ekstern IT-sikkerhedsanalyse, da det gør det lettere at kommunikere IT-sikkerhed og eventuel mangel på samme til ledelsen.

Erfaringsbaserede drivkræfter for øget IT-sikkerhed

Gennem Deloittes rådgivende arbejde med IT-sikkerhed i danske SMV'er er det tydeligt, at særligt fire årsager er dominerende i virksomhedernes beslutning om at øge deres IT-sikkerhed:

1. **IT-sikkerhedsangreb eller -brud**
   Virksomheden har oplevet et IT-sikkerhedsangreb eller -brud og har behov for hjælp til at øge deres IT-sikkerhed.

2. **Ledelsesfokus og usikkerhed omkring IT-sikkerhedsniveau og -kompetence**
   Ledelsen henvender sig, fordi de er usikre på deres IT-sikkerhedsniveau, og erkender, at de ikke selv har de nødvendige kompetencer til at analysere dette. De kontakter derfor en ekstern rådgiver med henblik på at få undersøgt virksomhedens IT-sikkerhedsniveau. Generelt er der kommet større fokus på IT-sikkerhed på bestyrelsesniveau, hvilket i særlig grad skyldes, at truslen er steget markant de seneste to år, og at emnet italesættes i forskellige netværk, som bestyrelsesmedlemmer deltager i.

3. **Cyberforsikring**
   Man kan som virksomhed i dag tegne en cyberforsikring. I den forbindelse får forsikringsselskaberne lavet en IT-sikkerheds-analyse, der identificerer huller i virksomhedens IT-sikkerhed, hvilket kan medvirke til, at virksomheden øger sin indsats på området.

4. **Leverandørkrav**
   Virksomhederne ønsker et højt IT-sikkerhedsniveau hos deres leverandører og outsourcingpartnere, og de kontakter en ekstern rådgiver for at sikre dette. Det giver samtidig leverandøren mulighed for at lukke identificerede huller.

VIDEN BLANDT MEDARBEJDERE OG IT-ANSVARLIGE ER CENTRALT FOR AT LØFTE IT-SIKKERHEDSNIVEAUET

IT-sikkerhed skal forankres i virksomhedskulturen, hvis medarbejderne skal bidrage til IT-sikkerheden

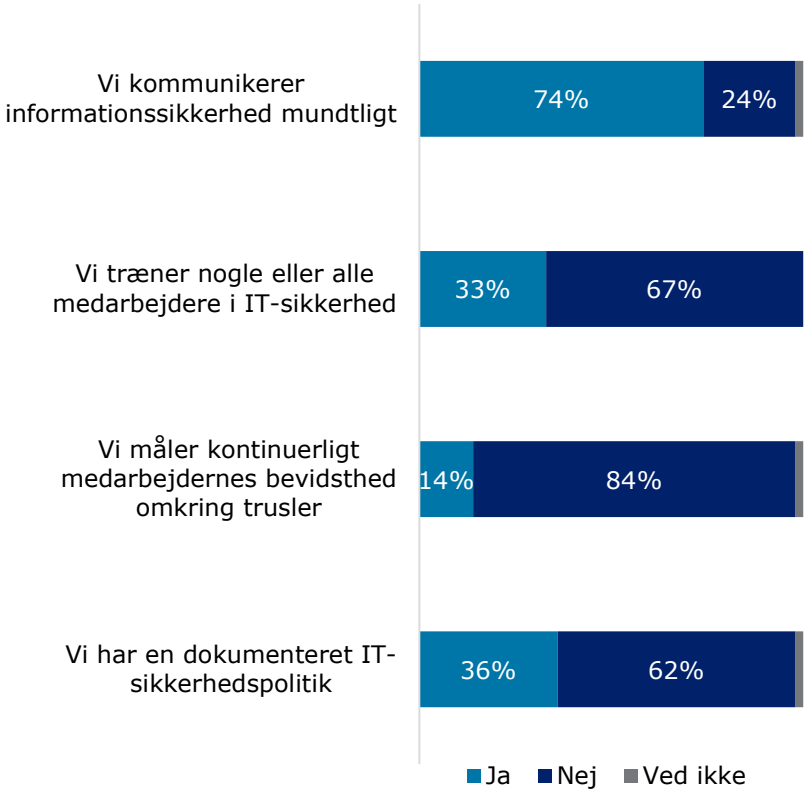
10 af de 14 casevirksomheder, som man kan læse om i rapporten *IT-sikkerhed og datahåndtering i danske SMV'er*, oplever medarbejdernes handlinger og manglende viden om IT-sikkerhed som en barriere for virksomhedens arbejde med IT-sikkerhed. Dette viser sig blandt andet ved, at medarbejderne har en manglende imødekommenhed overfor forandringer eller ikke i tilstrækkelig grad er i stand til at identificere IT-sikkerhedstrusler, når de møder dem. Flere virksomheder nævner i den sammenhæng virksomhedskulturen som en underlæggende barriere for at øge IT-sikkerhedsniveauet i virksomheden. Flere IT-ansvarlige mener, det er nødvendigt at arbejde meget med kommunikation omkring IT-sikkerhed og potentielle IT-sikkerhedstrusler for at forankre IT-sikkerhed i virksomhedskulturen. Den uformelle kommunikation er i den sammenhæng et vigtigt redskab til at skabe den nødvendige kulturforandring gennem et øget fokus på IT-sikkerhed og en forståelse af vigtigheden af IT-sikkerhed samt ikke mindst konsekvenserne af manglende IT-sikkerhed for virksomheden/arbejdspladsen. Det er centralt, at medarbejderne forstår IT-sikkerhed, og det er derfor nødvendigt at gøre IT-sikkerhed til et mere håndgribeligt koncept og sørge for, at IT-sikkerhed målrettes de enkelte medarbejdergrupper.

Virksomhederne kan implementer forskellige IT-sikkerhedstiltag målrettet medarbejderne, som er formaliserede i varierende grad. Der ses en tendens til, at virksomhederne især anvender ikkeformaliserede tiltag, og at færre virksomheder anvender formaliserede tiltag.

Eksempelvis er det hele 74 procent af de danske SMV'er, der kommunikerer deres informations-sikkerhed mundtligt. Den mundtlige kommunikation er en ikkeformaliseret måde at øge medarbejderens viden om informationssikkerhed på, og det er en stor del af virksomhederne, der anvender denne tilgang. Modsat er der færre virksomheder, der anvender formaliserede IT-sikkerhedstiltag målrettet medarbejderne. Det er især en lille del af virksomhederne, der måler på medarbejdernes bevidsthed om IT-sikkerhedstrusler.

Årsagen til, at få virksomheder anvender formaliserede IT-sikkerhedstiltag, kan være, at virksomhederne starter deres arbejde med IT-sikkerhed med den mundtlige kommunikation, hvorefter mere formaliserede tiltag bygges på. Graden af formalisering af virksomhedens tiltag på området har en stor sammenhæng med virksomhedens samlede IT-sikkerhed. 92 procent af virksomhederne med 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 er det kun 15 procent, der har en dokumenteret IT-sikkerhedspolitik, og kun 5 procent måler på medarbejdernes bevidsthed om IT-sikkerhedstrusler.

Figur 6. IT-sikkerhedstiltag relateret til medarbejdere



Note: Figuren viser den vægtede andel af SMV'er, der har implementeret IT-sikkerhedstiltag målrettet medarbejderne.
Kilde: Wilke for Monitor Deloitte.

Viden om IT-sikkerhed er central for SMV'ernes arbejde med IT-sikkerhed

I flere virksomheder er det en barriere for igangsættelse af nødvendige IT-sikkerhedsforanstaltninger, at den IT-ansvarlige ikke har viden om trusselsbilledet, og hvilke produkter og løsninger der er på markedet. Hvis virksomhedens IT-ansvarlige ikke har tilstrækkelig viden, er arbejdet med IT-sikkerhed svært, fordi man ikke har det fuldstændige billede. Dette kan medføre, at virksomheden ikke vurderer sin IT-sikkerhed på et tilstrækkeligt videngrundlag.

En væsentlig kilde til viden om IT-sikkerhed er professionelle og personlige netværk og fora

Fem ud af 14 interviewede virksomheder 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. Her findes der brancherelaterede fora, men også fora, der er tværgående og forener flere aktører. 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.

IT-SIKKERHED SOM EN DEL AF VIRKSOMHEDSKULTUREN HOS TP AEROSPACE

Om virksomheden

Navn | TP Aerospace

Branche | Engroshandel og detailhandel

Størrelse | 220 medarbejdere

TP Aerospace sælger flyhjul og -bremser til mindre fly- og fragtselskaber og henvender sig til internationale markeder. TP Aerospace har syv lokationer globalt og har siden virksomhedens etablering i 2008 haft en betydelig vækst hvert år.

Virksomhedens IT-anvendelse

Virksomheden opbevarer personaledata og kundeinformationer, men ingen direkte personfølsomme data. Derudover har de et databasesystem med oversigt over varer. En læk af data vil ikke få konsekvenser, men en eventuel kryptering vil have betydning for forretningen.

Indtil 2016 havde TP Aerospace udelukkende brugt eksterne IT-konsulenter, men de vurderede på det tidspunkt, at de var nødt til at have interne IT-kompetencer. Årsagen hertil var først og fremmest, at det blev nødvendigt at have et internt talerør – en, der kunne omsætte IT til noget forståeligt i organisationen – men det var dog ikke udelukkende af IT-sikkerhedsmæssige grunde, man ansatte en IT-ansvarlig. Da den nye IT-ansvarlige startede i virksomheden, påbegyndte han arbejdet med IT-sikkerhed og startede helt fra bunden med at indføre password på medarbejdernes pc'er. I processen med at øge IT-sikkerhedsniveauet har medarbejdernes handlinger og begrænsede viden om IT og IT-sikkerhed været en barriere for arbejdet med IT-sikkerhed, da der var en modvilje mod de forandringer, der var nødvendige. Da den nye IT-ansvarlige for eksempel indførte password på alle medarbejderes pc'er, havde de svært ved at forstå nødvendigheden heraf. Derfor brugte den IT-ansvarlige meget af sin tid på at kommunikere de forandringer, der fulgte i relation til IT-sikkerhed, herunder informere medarbejderne, inden forandringerne blev implementeret, og forklare, hvorfor forandringerne var nødvendige. IT-afdelingen udarbejdede for eksempel et nyhedsbrev og en blog, hvor man satte fokus på IT-sikkerhed.

Den IT-ansvarlige oplevede, at arbejdet med IT-sikkerhed ikke blot handlede om at implementere nye IT-sikkerhedsforanstaltninger – det krævede også en kulturændring blandt medarbejderne i forhold til at skabe en større forståelse af IT og gøre IT-sikkerhed til en mere naturlig del af arbejdet; i særlig grad for at sikre, at medarbejderne var opmærksomme på eventuelle IT-sikkerhedstrusler som for eksempel et phishingangreb. Den indledende tilgang til IT og IT-sikkerhed, hvor medarbejdere eller ledelse havde begrænset opmærksomhed omkring IT-sikkerhed, havde været en del af virksomheden siden dens etablering, hvorfor det var så dybt forankret i kulturen.

TP Aerospaces kunder kræver, at virksomheden har en række certificeringer; disse auditeres løbende. TP Aerospace har oplevet, at auditeringerne går nemmere, fordi virksomheden kan dokumentere sin IT-sikkerhed. Det har for TP Aerospace også betydet, at de udarbejder separate beskrivelser af IT-sikkerheden, som er specifikt målrettet auditørerne.

Udover den generelle sikring af virksomhedsdriften er TP Aerospaces arbejde med IT-sikkerhed i høj grad drevet af, at den IT-ansvarlige igennem netværk og medier holder sig opdateret om IT-sikkerhed, og ved, hvad der rører sig på området.

Hos TP Aerospace ser den IT-ansvarlige det som centralt at tilegne sig viden om IT-sikkerhed og ikke mindst sparre og erfaringsdele med andre virksomheder omkring IT-sikkerhed. Det ses som værende særlig centralt at høre andres erfaringer for bedre selv at kunne navigere i produkter og IT-sikkerhedsløsninger.

> *Jeg bruger tid på at forklare medarbejderne, hvilke forandringer jeg laver, og hvorfor de er nødvendige*

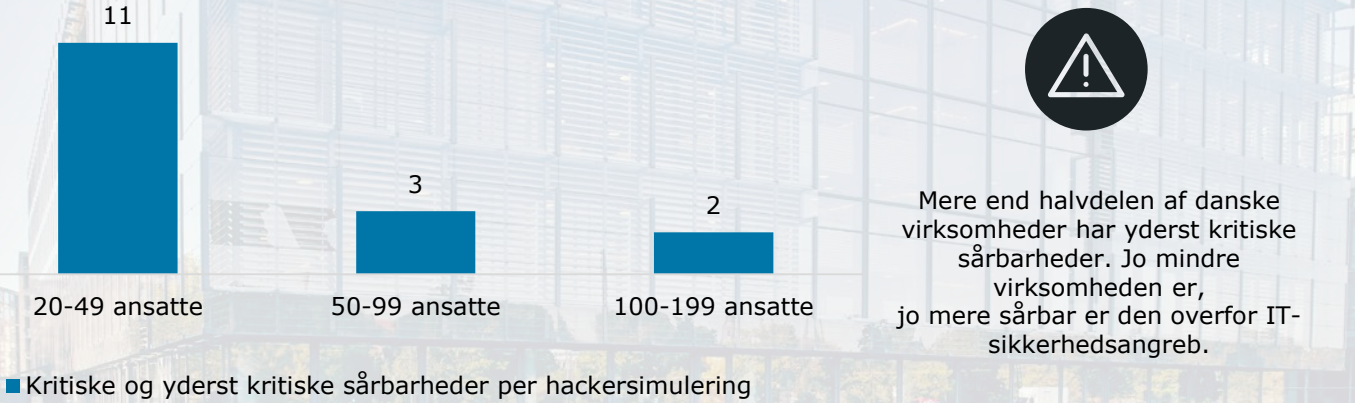
TP Aerospaces egen refleksion på baggrund af deres oplevelser med IT-sikkerhed.

HACKERSIMULERINGER BEKRÆFTER, AT EN STOR ANDEL AF VIRKSOMHEDERNE ER SÅRBARE

Mange virksomheder har ikke et tilstrækkeligt IT-sikkerhedsniveau i forhold til deres risikoprofil og er derfor sårbare overfor IT-sikkerhedsangreb. Hackersimuleringer er en måde at teste en virksomheds tekniske IT-sikkerhedsniveau på. Deloitte Cyber Risk har siden 2012 gennemført flere tusind hackersimuleringer i over 550 danske virksomheder.

Ser man på tværs af de virksomheder, der er blevet testet af Deloitte Cyber Risk, har 57 procent af virksomhederne haft yderst kritiske sårbarheder. Når man ser på tværs af alle sårbarheder, er 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, som det ses i figur 7. Mindre virksomheder er specielt udsatte, da de i mindre grad har kompetencer på området i forhold til større virksomheder. Det skyldes ofte manglende økonomiske ressourcer, da dygtige IT-sikkerhedsfolk er dyre. Ofte kan de små virksomheder heller ikke tiltrække de dygtige folk.

Figur 7. Antal gennemsnitslige kritiske sårbarheder ved seneste sikkerhedsscanning



Kilde: IT-sikkerhed og datahåndtering i danske SMV'er

Hvis der er sårbarhed i et forretningskritisk system, vil en hacker i værste fald kunne kompromittere systemet og få adgang til forretningskritiske data eller påvirke tilgængeligheden og dermed medføre nedetid for virksomhedens drift. Kritiske sårbarheder i et system kan potentielt også medføre yderligere kompromittering af andre systemer i netværket, der ellers ikke var direkte tilgængelige. Hvis en angriber opnår adgang til data, kan disse krypteres, som det for eksempel ses med ransomwareangreb, eller alternativt lækkes økonomiske data med store imagetab til følge. Sidstnævnte bliver særlig interessant efter 25. maj 2018, hvor persondataforordningen træder i kraft.

Hackersimuleringerne ser 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 mv.) 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 funktionaliteter, der kan udnyttes af uautoriserede.

Database. Denne kategori omhandler den bagvedliggende database. Det kan for eksempel være sårbarheder som SQL injection, e-nummerering af databaseopslag, fingerprinting af databaseversion og type mv.

ANTALLET AF IT-SIKKERHEDSBRUD ER STÆRKT STIGENDE OG KAN HAVE STORE KONSEKVENSER

Undersøgelsen peger på, at cirka 14 procent af danske SMV'er på et tidspunkt har oplevet et IT-sikkerhedsbrud, men tallet kan være højere.

På landsplan svarer det til, at cirka 11.000 danske SMV'er har oplevet et IT-sikkerhedsbrud. Heraf har 43 procent haft et IT-sikkerhedsbrud indenfor det seneste år, svarende til 4.700 SMV'er.

Det præcise tal for IT-sikkerhedsangreb og IT-sikkerhedsbrud er dog forbundet med stor usikkerhed og er dermed vanskeligt at estimere. Dette skyldes blandt andet, at mange virksomheder ikke ønsker at dele information om IT-sikkerhedsbrud. Dertil kommer, at mange virksomheder simpelthen ikke aner, at de har været ofre for et IT-sikkerhedsangreb. Denne usikkerhed betegnes mørketal. Der er tegn på, at flere end 14 procent af danske SMV'er har været ramt af et IT-sikkerhedsbrud. For eksempel har 35 procent af casevirksomhederne haft et IT-sikkerhedsbrud, og i PwC's Cybercrime Survey 2017 har 70 procent af respondenterne svaret, at de har været udsat for et IT-sikkerhedsangreb.

Da et IT-sikkerhedsbrud kan have omfattende konsekvenser for en virksomhed, er det iøjefaldende, at 39 procent af SMV'erne ikke har et tilstrækkeligt IT-sikkerhedsniveau. Konsekvenserne kan være direkte omkostninger relateret til at få forretningen op at køre igen efter et brud, men det kan også være mere langsigtede konsekvenser for virksomheden, der kan betyde, at virksomheden mister sit forretningsgrundlag, hvis for eksempel forretningskritiske data lækkes og på den måde kan kopieres af eller sælges til konkurrenter.

Størstedelen af de adspurgte SMV'er er afhængige af deres IT-systemer i deres daglige drift. Omtrent 60 procent af SMV'erne gemmer følsomme personoplysninger, 44 procent gemmer forretningskritiske data, og små 20 procent af SMV'erne nævner, at en læk af forretningskritiske data vil betyde, at de mister deres forretningsgrundlag og potentielt må dreje nøglen om. Et IT-sikkerhedsbrud, der for eksempel låser virksomhedens data eller giver adgang til centrale data, kan altså have vidtrækkende og skadende konsekvenser for mange danske SMV'er.

HVAD ER MØRKETAL?

Forskellen mellem den opdagede og uopdagede forekomst af IT-sikkerhedshændelser betegnes mørketal. IT-trusselsbilledet og det aktuelle omfang af IT-sikkerhedsangreb i Danmark er kompliceret at afdække. Dette skyldes blandt andet et manglende begrebsapparat på området, at man som virksomhed 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 IT-sikkerhedsangreb.

Det er ikke kun antallet af IT-sikkerhedshændelser, der er forbundet med stor usikkerhed. De omkostninger, der er forbundet med et IT-sikkerhedsbrud, er også svære at estimere. Denne undersøgelse peger på et gennemsnitligt omkostningsniveau ved et IT-sikkerhedsbrud på knap 40.000 kr. Af virksomhederne, der havde omkostninger forbundet med et brud, oplevede flere virksomheder omkostninger i størrelsesordenen 100.000-200.000 kr. Flere undersøgelser viser dog, at dette beløb sandsynligvis er højere, for eksempel PwC's Cybercrime Survey 2017, hvori de gennemsnitlige økonomiske omkostninger i forbindelse med et IT-sikkerhedsbrud opgøres til 900.000 kr. I sommeren 2017 oplevede Mærsk som skrækeksempel, at de samlede omkostninger ved et IT-sikkerhedsbrud løb op i 1.6 mia. kr.

IT-sikkerhedshændelser, -angreb og -brud

Et IT-sikkerhedsangreb er et forsøg på at kompromittere en virksomheds IT-systemer, for eksempel med det formål at få adgang til en virksomheds data eller sætte IT-systemer ud af drift. Hvis en virksomhed kan afværge angrebet, sker der ikke et IT-sikkerhedsbrud. Lykkes IT-sikkerhedsangrebet derimod, er der tale om et IT-sikkerhedsbrud, der kan få konsekvenser for virksomheden. Dette kan for eksempel være, hvis virksomhedens data krypteres af et ransomware-angreb, eller hvis angriberne får adgang til fortrolige data ved at hacke sig ind i virksomhedens systemer. Fællesbetegnelsen for IT-sikkerhedsangreb og IT-sikkerhedsbrud er IT-sikkerhedshændelser.

> 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.

Kilde: IT-sikkerhed og datahåndtering i danske SMV'er

ET IT-SIKKERHEDSBRUD ØGER OPMÆRKSOMHEDEN PÅ IT-SIKKERHED HOS AARHUS TEATER

Om virksomheden

Navn | Aarhus Teater

Branche | Kultur, forlystelser og sport

Størrelse | cirka 150 medarbejdere

Aarhus Teater opsætter teaterforestillinger og administrerer herunder selv forberedelse, opsætning og billetsalg.

Virksomhedens IT-anvendelse

Aarhus Teater er afhængigt af IT i deres daglige arbejde. Blandt andet lagrer teatret data vedrørende forestillinger, skuespillerne, kommende teaterprogrammer og manuskripter. Data vedrørende teatrets forestillinger betragtes som følsomme, og en læk af disse data ville være kritisk. Derudover er teatret meget afhængigt af et billetsystem, der er kritisk for forretningens daglige drift, da det er herigennem, omsætningen genereres. Derudover har teatret et økonomisystem og et HR-system, der opbevarer mindre kritiske data.

Aarhus Teater er det seneste år gået fra at have mange fragmenterede systemer til at samle det meste IT hos én leverandør. Dette for at omkostningsreducere, men også for at få bedre service og adgang til en større supportafdeling og ikke mindst et øget niveau af IT-sikkerhed.

I februar 2017 oplevede Aarhus Teater et IT-sikkerhedsbrud. En medarbejder var utilsigtet kommet til at trykke på et link og på den måde lukke ubudne gæster ind i IT-systemerne på Aarhus Teater. Ved hurtigt at lokalisere kilden til sikkerhedsbruddet begrænsede Aarhus Teater konsekvenserne, så kun 11.000 af 300.000 filer blev krypteret. I samarbejde med virksomhedens partnere, fik man løst problemet, men virksomheden kunne ikke bruge IT i knap fire dage.. Efterfølgende er der ingen umiddelbare tegn på langvarige konsekvenser, da det ikke tyder på, at Aarhus Teater mistede filer i forbindelse med IT-sikkerhedsbruddet, idet ingen aktivt har meldt ud, at de mangler filer.

Aarhus Teater er en kreativ virksomhed, hvor medarbejderne ikke nødvendigvis har daglig berøring med og stor viden om IT, hvilket skabte udfordringer for kommunikationen, og den IT-ansvarlige oplevede, at det kunne være svært at forene kreativiteten i huset med fokus på IT-sikkerhed.

IT-sikkerhedsbruddet blev derfor brugt aktivt til at sætte IT-sikkerhed på dagsordenen og skabe forståelse af arbejdet med at skabe IT-sikkerhed i medarbejdernes daglige rutiner. IT-sikkerhedsbruddet betød, 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.

Aarhus Teater har outsourcet en del af deres IT. Dette giver adgang til en større supportfunktion, end virksomheden har mulighed for at drive selv. Samtidig oplever teatret, at outsourcing – og især samling af IT på én platform – øger IT-sikkerheden på væsentlige parametre. Via outsourcing får IT-afdelingen adgang til specifikke kompetencer, som de ikke besidder internt, men det betyder også, at medarbejderne ikke selv kan installere programmer og systemer på deres pc'er, hvilket minimerer risikoen for, at der downloades uhensigtsmæssige programmer mv.

Virksomheden har oplevet, at medarbejderne selv er begyndt at tænke over IT-sikkerhed og komme med forslag til nye tiltag, f.eks. hvordan man kan streame optagelser af en forestillingsprøve til en person, der sidder et andet sted i landet. Aarhus Teater ser dette som en positiv udvikling og som et udtryk for, at medarbejderne engagerer sig mere i IT-sikkerhed.

> *Hvis alle medarbejdere var opmærksomme på IT-sikkerhed, behøvede vi næsten ikke andre tiltag mod phishingmails.*

Aarhus Teaters egen refleksion på baggrund af deres oplevelser med et IT-sikkerhedsbrud

at AARHUS TEATER

TIL VIRKSOMHEDSLEDEREN: HAR DIN VIRKSOMHED TAGET STILLING TIL IT-SIKKERHED?

Du bør vurdere din virksomheds IT-sikkerhedsniveau i relation til din virksomheds IT-anvendelse og risikoprofil. En virksomheds anvendelse af IT og lagring af data har indflydelse på, hvilke konsekvenser et IT-sikkerhedsbrud kan have, og ikke mindst sandsynligheden for at blive ramt af et IT-sikkerhedsbrud. IT-anvendelse og lagring af følsomme data er de vigtigste parametre i din virksomheds risikoprofil, og din virksomheds IT-trusselsbillede hænger tæt sammen med din virksomheds risikoprofil.

Det er derfor afgørende, at du klarlægger din virksomheds risikoprofil ved at vurdere, hvor afhængige I er af jeres IT-systemer, og i hvilken grad I lagrer følsomme data, inden du igangsætter en eventuel styrkelse af din virksomheds IT-sikkerhedsniveau. Du kan få et hurtigt overblik over din risikoprofil og IT-sikkerhedsniveau ved at svare på nedenstående spørgsmål.

Kan du svare **ja** til et eller flere af spørgsmålene i boksen med overskriften *Risikoprofil* og **nej** til et eller flere af spørgsmålene i boksen med overskriften *IT-sikkerhedsniveau* nedenfor, kan din virksomhed være sårbar overfor IT-sikkerhedsangreb og har dermed en øget risiko for et reelt IT-sikkerhedsbrud. Kender du ikke svaret, kan det være værd at overveje at sætte sig bedre ind i virksomhedens IT-sikkerhed.

Risikoprofil

- Er din virksomhed afhængig af IT-systemer i den daglige drift?
- Håndterer og gemmer din virksomhed følsomme personoplysninger (fx informationer om personers køn, seksualitet, politiske overbevisning, etnicitet)?
- Håndterer og gemmer din virksomhed forretningskritiske data (fx patentansøgninger og intellektuelle rettigheder)?
- Tilhører din virksomhed en særlig udsat branche (fx den finansielle sektor).

IT-sikkerhedsniveau

- Har din virksomhed opdateret systemer og programmer indenfor den seneste måned?
- Har din virksomhed dokumenterede og gennemtestede backupprocedurer?
- Har din virksomhed en IT-sikkerhedspolitik, og er den blevet revideret indenfor det seneste år?
- Foretager din virksomhed løbende IT-risikovurderinger?
- Uddanner og træner din virksomhed medarbejderne i IT-sikkerhedstrusler og sikker databehandling?

Hvis din virksomhed mangler hjælp eller yderligere information til at arbejde med IT-sikkerhed og databeskyttelse, kan du blandt andet finde mere information her:

Sikkerhedstjekket

Sikkerhedstjekket giver overblik over, om der er svagheder i jeres IT-sikkerhed og yder målrettet vejledning i, hvor der bør sættes ind først for at mindske risikoen for at blive ramt af et IT-sikkerhedsangreb. Se mere på www.sikkerhedstjekket.dk.

PrivacyKompasset

PrivacyKompasset er en hjælp til danske virksomheder. Det tilbyder vejledning i reglerne om persondatabeskyttelse og giver mulighed for at generere en skræddersyet privatlivspolitik. Privatlivspolitikken kan let formidles til kunder og samarbejdspartnere og bidrager til den digitale tillid. Se mere på www.privacykompasset.dk.

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 264.000 medarbejdere gør en forskel, der betyder noget, så besøg os på Facebook, LinkedIn eller Twitter.

Monitor
Deloitte.