Forankring af IT-sikkerhed i virksomhedens ledelse

IT-sikkerhed er relevant for hele virksomheden uanset størrelse. Derfor er det vigtigt, at ledelsen er involveret i opgaven med at formulere og skabe IT-sikkerhed. Ansvaret tilhører i sidste ende ledelsen. Det er ledelsens opgave at vurdere, hvor stor en IT-sikkerhedsmæssig risiko, virksomheden kan acceptere. Derfor er det også ledelsen, som skal prioritere ressourcer til at øge sikkerheden. Ledelsen er et eksempel til efterfølgelse blandt medarbejderne. Derfor er det vigtigt, at ledelsen både viser og kommunikerer til medarbejderne, at IT-sikkerhed er noget, der skal være fokus på.

Anbefalinger til, hvad ledelsen skal gøre for at styrke IT-sikkerheden

- Ledelsen påtager sig ansvar og optræder som rollemodel i forhold til virksomhedens arbejde med IT-sikkerhed.
- Ledelsen tager aktivt stilling til IT-sikkerhedsmæssige risici og virksomhedens risikovillighed.
- Ledelsen sikrer løbende styring af virksomhedens arbejde med IT-sikkerhed.

Ledelsen påtager sig ansvar og optræder som rollemodel i forhold til virksomhedens arbejde med IT-sikkerhed

Ledere bør gennem deres handling og kommunikation vise medarbejderne, hvor vigtigt det er, at alle i virksomheden er opmærksomme på IT-sikkerhed. Hvis virksomheden fx indfører nye procedurer, der kan gøre det daglige arbejde mere besværligt for at øge sikkerhedsniveauet, er det vigtigt, at ledelsen er med til at kommunikere behovet og baggrunden for disse procedurer. Det er ikke IT-afdelingen, som skal stå på mål for ændringerne. Det er vigtigt, at ledelsen er synlig og deltager i en løbende indsats for at øge medarbejdernes bevidsthed om IT-sikkerhed. Der findes mange måder at gennemføre sådanne indsatser. På Erhvervsstyrelsens kampagneside Klik ikke her finder du gratis materiale og gode råd, der kan bruges til at oplyse medarbejdere om IT-sikkerhed.

Ledelsen tager aktivt stilling til virksomhedens IT-sikkerhedsmæssige risici og virksomhedens risikovillighed

For at kunne afgøre, hvor højt sikkerhedsniveauet bør være, er det nødvendigt at lave en vurdering af risikoen. Det giver et overblik over, hvor virksomheden er mest sårbar, og hvad der kan gøres for at reducere sårbarheden. Det er også vigtigt at tage stilling til, hvor stor risiko der anses for at være acceptabel. Ingen virksomhed kan være 100 procent sikker.

Se også Anbefaling 3 – Lav en risikovurdering.

Ledelsen sikrer løbende styring af virksomhedens arbejde med IT-sikkerhed

For at sikre, at IT-sikkerhedsarbejdet når hele vejen rundt i virksomheden, kan det være en fordel at have en IT-sikkerhedspolitik, som skaber rammerne for virksomhedens arbejde med IT-sikkerhed.

Se også Anbefaling 4 – IT-sikkerhedspolitik.

Hvis du er IT-sikkerhedsansvarlig, er der konkrete forslag til, hvordan du sætter ord på IT-sikkerhed overfor resten af ledelsen på SikkerDigital.

Få overblik over virksomhedens mest værdifulde data og kritiske systemer

Når I skal styrke IT-sikkerhedsniveauet er det vigtigt først at kortlægge virksomhedens vigtigste data, informationer og de systemer, som håndterer dem. Alle virksomheder er forskellige og håndterer mange forskellige typer af informationer. Det kan blandt andet være oplysninger om kunder og medarbejdere, økonomiske nøgletal, viden om opgaver, leverancer, produktion, distribution, kontrakter, aftaler, CRM-systemer osv. Det er afgørende, at I tager stilling til, hvilke informationer og IT-systemer der er vigtigst for netop jeres virksomhed. Så kan I bedre sætte ind, hvor det er nødvendigt og bruge jeres ressourcer mest optimalt.

Anbefalinger til at skabe overblik over virksomhedens mest værdifulde data og kritiske systemer

- Få overblik over personoplysninger.
- Få overblik over forretningskritiske data.
- Få overblik over kritiske systemer.

Et overblik indebærer, at der indsamles viden fra hele virksomheden (fx system- og dataejere), og at overblikket skrives ned og løbende opdateres.

Få overblik over personoplysninger

Det er vigtigt, at I får overblik over hvilke typer personoplysninger, I håndterer i jeres virksomhed, da databeskyttelsesforordningen sætter retningslinjer for behandling og opbevaring af personoplysninger. Både informationer om jeres kunder og om medarbejderne i virksomheden er vigtige at tage stilling til.

Se hvordan i Anbefaling 5 – håndtering af personoplysninger

På PrivacyKompasset kan du finde en online test, der skal hjælpe virksomheder i gang med at efterleve databeskyttelsesreglerne og få svar på helt basale spørgsmål i forhold til ansvarlig datahåndtering.

Få overblik over forretningskritiske data

I kortlægningen af jeres virksomheds mest værdifulde og forretningskritiske informationer og data, kan det være en hjælp at involvere fx ledere eller andre i virksomheden, som har mere specifik viden om eller ejerskab over forskellige typer af data og viden i virksomheden.

Eksempler på forretningskritiske data:

- Informationer, som er afgørende for at holde jeres produktion i gang.
- Kundeinformation.
- Forretningshemmeligheder og patenter.
- Økonomiske nøgletal og prisstrategi.

Få overblik over kritiske IT-systemer

Det er også vigtigt at få overblik over de vigtigste systemer, som håndterer virksomhedens informationer. For at vurdere, hvilke systemer I er mest afhængige af, kan I tage udgangspunkt i hvor lang tid det tager, før manglende systemadgang bliver et problem for jeres virksomhed:

- **Kritisk** - under 4 timer: Manglende adgang til systemer vil skade virksomheden næsten med det samme, fordi I ikke kan producere eller levere jeres ydelser til kunderne.
- **Modera**t - 4-8 timer: Manglende adgang må helst ikke vare mere end en enkelt arbejdsdag, før det begynder at skade virksomheden.
- **Lav** - under en uge: Virksomheden kan godt undvære adgang til systemer i op til en uge, men helst ikke mere.
- **Meget lav** – en uge eller længere: Virksomheden kan undvære et eller flere systemer i en uge eller mere. Det kan fx være støttesystemer, som ikke anvendes på daglig basis.

Når I har fået overblik over, hvilke vigtige IT-systemer I har i jeres virksomhed, skal ledelsen beslutte, hvem der er system- og procesansvarlig for hvert enkelt system. Det er den system- eller procesansvarlige, der skal sikre at systemerne løbende bliver opdateret og vedligeholdt.

Lav en risikovurdering

Den øgede digitalisering øger risikoen for, at jeres virksomhed kan blive ramt af forskellige typer digitale angreb eller andre trusler, som kan skade virksomhedens økonomi, omdømme og konkurrenceevne.

Det er oftest billigere at forebygge fremfor at skulle reparere, når I skaden er sket.

En risikovurdering af jeres virksomhed giver jer det nødvendige overblik over, hvad I har af risici, så I målrettet kan arbejde på at minimere dem.

- Du kan finde et værktøj til at lave en risikovurdering for jeres virksomhed her

Anbefalinger til at lave en risikovurdering

For at lave en målrettet risikovurdering og handleplan, skal I tage stilling til disse spørgsmål:

- Hvilke trusler kan ramme jer?
- Hvad er sandsynligheden for, at I rammes?
- Hvad er konsekvenserne, hvis I rammes?
- Hvordan sikrer I jer mod de største risici?

1

Hvilke trusler kan ramme jer?

Der findes mange typer trusler, som kan ramme danske virksomheder, og der kommer hele tiden nye trusler. De IT-kriminelles metoder udvikler sig i takt med den teknologiske udvikling.

Nogle af truslerne er meget almindelige og vil kunne ramme de fleste danske virksomheder. Det kan fx være virus eller ransomware, som sendes ud med phishingmails til en stor gruppe modtagere. Andre trusler kan jeres virksomhed være særligt udsatte for, hvis I fx ligger inde med værdifulde data, som IT-kriminelle kan være motiverede for at stjæle. Det er en god ide at danne sig et overblik over både de generelle trusler og de specifikke trusler, som virksomheden er særligt udsat for.

Se mere om trusselsbilledet her.

2

Hvad er sandsynligheden for, at I rammes?

Det kan være vanskeligt at vurdere, hvor sandsynligt det er, at jeres virksomhed bliver et mål for IT-kriminelle. Sandsynligheden kan fx udtrykkes på en skala fra 1-5:

1 - Sjælden eller usandsynlig.
2 - Vil næppe forekomme.
3 - Er mulig.
4 - Må forventes at kunne ske.
5 - Vil blive udnyttet.

3

Hvad er konsekvensen, hvis I rammes?

Næste trin i risikovurderingen handler om at vurdere de forretningsmæssige konsekvenser ved, at jeres virksomhed bliver ramt. Konsekvenserne kan fx have betydning for virksomheden omdømme, kundernes tillid, jeres økonomi, tabt arbejdstid eller manglende overholdelse af lovgivning.

Jo større og mere alvorlige konsekvenserne er, jo vigtigere er det at fokusere sit sikkerhedsarbejde. Konsekvenser kan fx vurderes på en skala fra 1-5:

1 - Meget lille konsekvens – det har reelt ikke nogen betydning.
2 - Lille konsekvens – det kan håndteres som en del af driften.
3 - Nogen konsekvens – der er behov for ekstra ressourcer.
4 - Høj konsekvens – det har betydning for bundlinjen.
5 - Meget stor konsekvens – firmaet er truet.

4

Hvordan sikrer I jer mod de største risici?

Når I har identificeret de væsentligste trusler og konsekvenserne, vil det næste trin være at undersøge, om virksomheden har de nødvendige sikkerhedsforanstaltninger. Ligesom risikobilledet er forskelligt fra virksomhed til virksomhed, er der også forskel på, hvilke sikkerhedsforanstaltninger som er relevante for jeres virksomhed.

En god tommelfingerregel kan være, at virksomhedens sikkerhedsforanstaltninger skal svare til den risiko, virksomheden står overfor.

Se en oversigt over de teknologiske og organisatoriske sikkerhedsforanstaltninger, som I bør overveje at implementere her.

Anbefaling 4 - Få en IT-sikkerhedspolitik

Hvorfor er det vigtigt?

Der er flere gode grunde til, at have en nedskrevet IT-sikkerhedspolitik, som både ledelse og medarbejdere kender. Det er her, virksomheden opridser sin tilgang til IT-sikkerhed. En IT-sikkerhedspolitik kan blive udleveret til nye medarbejdere og bruges som opslagsværk for medarbejdere, som er i tvivl om, hvordan de skal forholde sig til IT-sikkerhed.

En IT-sikkerhedspolitik kan på den måde være med til at:

- **Skabe klare retningslinjer** - En nedskrevet IT-sikkerhedspolitik giver både ledelse og medarbejdere klare retningslinjer for, hvad der forventes i forhold til IT-sikkerhed.
- **Styrke virksomhedens omdømme** - Fokus på IT-sikkerheden styrker virksomhedens troværdighed, både hos jeres kunder og jeres samarbejdspartnere.
- **Mindske sårbarhed når IT-medarbejdere stopper** – Når I har skrevet de vigtigste retningslinjer ned sikres det, at det ikke blot er kernemedarbejderen med ansvaret for IT og IT-sikkerhed, som har styr på hvordan I sikrer jeres digitale værdier.

Sådan kommer du i gang med at lave en IT-sikkerhedspolitik:

Afklar jeres behov

En IT-sikkerhedspolitik behøver ikke fylde flere ringbind – det vigtigste er, at den er tilpasset jeres specifikke virksomhed. Det bør være et dokument, der aktivt kommunikeres til alle medarbejdere og løbende opdateres.

For at finde ud af, hvor omfattende en IT-sikkerhedspolitik I har brug for, kan det være en fordel først at skabe sig et overblik over, hvilke data og systemer, der er særligt vigtige for driften af virksomheden.

Se mere om, hvad det indebærer, i Anbefaling 2 – Få overblik over virksomhedens mest værdifulde data og kritiske systemer.

Det kan også overvejes, om I skal tage udgangspunkt i en konkret risikovurdering. Læs mere om risikovurderinger i Anbefaling 3 – Lav en risikovurdering.

Kom i gang med at lave en IT-sikkerhedspolitik

Der er flere måder at lave en IT-sikkerhedspolitik på. På SikkerDigital kan du finde en skabelon, der kan bruges som udgangspunkt for at lave en IT-sikkerhedspolitik til jeres virksomhed.

En god tommelfingerregel er, at IT-sikkerhedspolitikken bliver mere vigtig for virksomheden, hvis der er mange medarbejdere. Men også mindre virksomheder bør tage stilling til, hvad deres behov er.

Anbefaling 5 - Håndtering af personoplysninger

Håndtering af personoplysninger

Med den nye databeskyttelsesforordning (GDPR) er der kommet ekstra fokus på virksomheders behandling af personoplysninger. Forordningen er med til at understøtte privatlivets fred som en fundamental rettighed indenfor EU. Loven har således til formål at beskytte borgerne mod misbrug af deres personoplysninger. Virksomheder, som ikke lever op til databeskyttelsesreglerne, kan tildes bøder på op til 20 mio. euro.

Reglerne for databeskyttelse gælder for al automatisk eller elektronisk behandling af personoplysninger. Det betyder, at så snart du er i kontakt med personoplysninger fra en kunde, medarbejder eller samarbejdspartner, så tæller det som behandling af personoplysninger.

Anbefalinger til håndtering af personoplysninger

- Find ud af, hvilke typer af personoplysninger, I håndterer
- Afklar jeres rolle
- Undersøg om behandlingen af personoplysninger lever op til forpligtelserne i databeskyttelsesreglerne.
- Test din virksomhed med PrivacyKompasset.

Find ud af hvilke typer personoplysninger I håndterer

Næsten alle virksomheder behandler personoplysninger af en eller anden slags. Det kan fx være oplysninger om medarbejdere (fx lønoplysninger, helbredsoplysninger eller fagforeningsmæssigt tilhørsforhold) eller kunder (fx kontaktoplysninger, adresser osv.).

Det er en fordel, hvis I tager udgangspunkt i, hvilke typer af personoplysninger I behandler. Det kan være:

- Almindelige personoplysninger
- Følsomme personoplysninger
- Oplysninger om strafbare forhold

Se mere om de forskellige typer af personoplysninger.

Afklar jeres rolle

I skal være opmærksomme på, hvilken rolle I spiller i forbindelse med databehandling. Om I er dataansvarlig, databehandler eller deler dataansvaret har betydning for, hvilke krav I skal leve op til.

Se mere om, hvordan I kan afklare jeres rolle som enten dataansvarlig eller databehandler.

Undersøg om behandlingen af personoplysninger lever op til de krav, der er i databeskyttelseslovgivningen

Som dataansvarlig er der en række forpligtelser i databeskyttelsesreglerne. En dataansvarlig skal for det første altid efterleve de grundlæggende krav til lovlig behandling af personoplysninger. De er:

1. Lovlighed, rimelighed og gennemsigtighed: Behandlingen skal overholde databeskyttelsesreglerne og være gennemsigtig
2. Formålsbegrænsning: Ved indsamling skal det være klart, hvilke saglige formål oplysningerne skal anvendes til. Senere behandling må ikke være uforenelig med disse formål
3. Dataminimering: Behandling, herunder opbevaring af oplysninger, skal begrænses til det, der er nødvendigt for at opfylde formålet
4. Rigtighed: Oplysninger skal ajourføres, og urigtige oplysninger skal slettes eller berigtiges
5. Opbevaringsbegrænsning: Når det ikke længere er nødvendigt at behandle oplysningerne, skal de anonymiseres eller slettes
6. Integritet og fortrolighed: Oplysninger må ikke komme til uvedkommendes kendskab, gå tabt eller blive beskadiget

For alle 6 principper gælder et grundlæggende princip: Ansvarlighed. Dvs. det skal kunne dokumenteres, at man efterlever de ovenstående principper.

For det andet skal den dataansvarlige sikre at den person, som oplysningerne vedrører, kan udleve en række rettigheder. Der skal således oplyses om, hvilken behandling der foregår med hvilke formål og på hvilke kategorier af personoplysninger. Desuden har personen ret til at søge indsigt og under visse omstændigheder ret til at få berigtiget eller slettet sine oplysninger m.v.

For det tredje skal den dataansvarlige efterleve en række pligter. Disse består bl.a. i at beskytte personoplysningerne ved at implementere passende sikkerhedsforanstaltninger, der passer til risici, at rapportere sikkerhedsbrud til myndighederne, at designe sine it-systemer så reglerne i forordningen understøttes og at styre og sikkerheden hos databehandlerne gennem en databehandleraftale. Se Anbefaling 17 – Lav en databehandleraftale.

Endelig skal de dataansvarlige være opmærksom på, om de behandler personoplysninger udenfor EU. I givet fald skal man finde et retligt grundlag for at gøre det.

Test din virksomhed med PrivacyKompasset

På PrivacyKompasset kan du finde en online test, der skal hjælpe virksomheder i gang med at efterleve databeskyttelsesreglerne og få svar på helt basale spørgsmål i forhold til ansvarlig datahåndtering.

PrivacyKompasset kan bruges til at:

- Få en status på, hvordan I håndterer personoplysninger i jeres virksomhed
- Få overblik over, hvad I skal gøre for at efterleve lovkravene

Yderligere information

På databeskyttelsesområdet er den centrale myndighed Datatilsynet. Find mere information om persondatabeskyttelse på Datatilsynets hjemmeside.

Anbefaling 6 - Fysisk IT-sikkerhed

Fysisk IT-sikkerhed

Tyveri eller tab af data foregår ikke altid elektronisk. Kriminelle kan forsøge at få adgang ved at møde op på virksomhedens adresse og prøve at bryde ind for at få adgang til computere eller serverrum. IT-systemer kan også blive beskadiget ved brand, vandskader eller hærværk. Derfor er det vigtigt at tænke fysisk sikkerhed ind i arbejdet med IT-sikkerhed.

Anbefalinger til fysisk sikkerhed

- Sikring mod indbrud.
- Beskyttelse mod oversvømmelse, ildebrand og stormskader.
- Nødstrøm og adgang til internet.

Sikring mod indbrud

Det er vigtigt, at I tager stilling til, hvor god jeres sikring mod indbrud er – og hvor sikker den skal være. Som minimum bør I have lås og alarmer på de udvendige døre. I kan også overveje at installere særligt sikrede skabe eller fjerne udstyr fra lokaler, når de forlades.

I kan også oprette ekstra sikrede zoner, hvis der er særligt følsomme data, som uvedkommende ikke må få adgang til. Det kan gøres med anlæg, der kontrollerer og begrænser adgangen, så det kun er særligt betroede medarbejdere, der har adgang til fx serverrum.

Hackere behøver ikke stjæle udstyret for at. Har de fysisk adgang, kan de fx sætte et USB-stik til jeres IT-udstyr, der tager kontrollen over jeres data – eller ødelægger dem. Derfor er det vigtigt, at alle i virksomheden er opmærksomme på, at uvedkommende ikke får mulighed for at færdes i virksomhedens lokaler.

Beskyttelse mod oversvømmelse, ildebrand og stormskader

Jeres IT-udstyr og data kan også blive udsat for vandskade, hvis der er oversvømmelse eller utætte rør. Overophedning, brand, torden eller stormvejr kan også ødelægge computere og slette data. Derfor bør I være opmærksomme på, hvordan I sikrer jer mod den slags skader, når I indretter jeres lokaler.

I kan fx sørge for, at jeres IT-udstyr står over vandlinjen for at undgå vandskader. Og det kan være en fordel at have udluftning og køling i serverrum for at undgå overophedning.

Nødstrøm og adgang til internet

Jeres IT-udstyr fungerer kun så længe, der er strøm til. Derudover er en stabil internetforbindelse ofte også nødvendig for, at IT-systemer virker, som de skal.

Til systemer, som det vil være meget kritisk ikke at have adgang til, kan I overveje at købe en nødstrømsforsyning. I kan også overveje, om jeres internetudbyder har en driftssikkerhed, som er tilstrækkelig ift. jeres behov.

Yderligere information om fysisk sikkerhed

Læs mere i vejledningen fra DI Digital til fysisk IT-sikkerhed.

Lav en beredskabsplan

Flere og flere virksomheder oplever brud på IT-sikkerheden. Derfor er det ekstra vigtigt, at der er en klar forståelse af, hvordan man skal reagere, hvis uheldet er ude. Medarbejdere og ledelse kan opleve et stort pres, når en IT-sikkerhedshændelse bliver opdaget. Derfor er det afgørende på forhånd at have klarhed over, hvem der gør hvad i hver enkelt situation.

Formålet med en beredskabsplan er at sikre, at jeres virksomhed reagerer hurtigt, målrettet og tilstrækkeligt, hvis I oplever en IT-sikkerhedshændelse. Dermed kan skaderne begrænses mest muligt.

Tre trin til et godt beredskab:

1) Lav en beredskabsplan:

En god beredskabsplan fastlægger de overordnede rammer for, hvordan jeres virksomhed håndterer IT-sikkerhedshændelser eller -brud.

På SikkerDigital kan I finde en skabelon for en beredskabsplan, som I kan tage udgangspunkt og tilpasse, så den passer til jeres virksomhed.

Det kan være en god idé at printe beredskabsplanen, da sikkerhedshændelser kan lamme systemer og funktioner, så I ikke kan komme til en digital version.

2) Stil krav til beredskabet hos jeres leverandører:

Et sikkerhedsbrud hos jeres IT-leverandører kan have stor betydning for jeres virksomhed. Hvis I fx bruger cloud-løsninger, er det cloud-leverandøren, der har opgaven og ansvaret for jeres datasikkerhed.

Derfor bør I aftale med jeres leverandører, hvordan deres beredskab er og stille sikkerhedskrav til dem.

Se også Anbefaling 16 – IT-sikkerhed hos jeres samarbejdspartnere.

3) Test jeres beredskab:

Det er vigtigt, at beredskabet ved IT-sikkerhedshændelser testes løbende (fx én gang om året). På den måde kan de ansvarlige træne i, hvordan de bedst udfylder den rolle, de har i beredskabsplanen. Og det er en god mulighed for at teste, om jeres beredskabsplan er god nok.

I kan lave en simpel ”skrivebordstest,” hvor de involverede personer gennemgår forskellige tænkte scenarier (fx et ransomware-angreb) og beskriver, hvad deres rolle er, hvad de skal gøre osv.

Hvis I gerne vil afprøve jeres beredskab, kan det også overvejes at købe en penetrationstest, hvor professionelle udsætter jer og jeres virksomhed for IT-sikkerhedsangreb.

Yderligere information

Her kan du læse Digitaliseringsstyrelsens vejledning til afprøvning og forbedring af beredskab

Her kan du læse Digitaliseringsstyrelsens vejlednig til IT-beredskab.

Medarbejdernes adgang til data og systemer

Mange virksomheder giver uden videre medarbejderne adgang til alle virksomhedens systemer. Det kan øge risikoen for, at virksomhedens data bliver tilgængelige for IT-kriminelle via en medarbejders computer. Fx hvis en medarbejder uforvarende kommer til at klikke på et virusinficeret link og dermed risikerer at give IT-kriminelle adgang til hele virksomhedens værdifulde data.

Medarbejdere, som bevidst tilegner sig fortrolige virksomhedsdata, er også en risiko. Læs mere om insidertruslen og hvad I kan gøre for at sikre jer i Anbefaling 9 – Insidertruslen.

For at beskytte virksomhedens data er det nødvendigt at begrænse medarbejdernes adgang, så medarbejderne kun har adgang til data, som er påkrævet i opgaveløsningen.

Anbefalinger til styring af medarbejderes adgang til data og systemer

- Få styr på adgangsrettigheder til data og systemer.
- Sikring af fjernadgang.
- Stil krav til sikkerheden i medarbejdernes adgangskoder.

Få styr på adgangsrettigheder til data og systemer

For at beskytte virksomhedens data er det en god ide at begrænse medarbejdernes adgang, så de kun har adgang til data og systemer, som er nødvendige i deres daglige arbejde. Det samme gælder administratorrettigheder. Disse bør kun tildeles medarbejdere, som har behov for dem.

På den måde undgår I, at medarbejdere ved en fejl ændrer opsætninger og gør systemerne mere sårbare for IT-kriminelle. Eller at hackere kan udnytte disse rettigheder, hvis en medarbejder bliver hacket. Medarbejdere bør ikke dele brugeradgang. Heller ikke hvis de fx bruger den samme computer.

Udpeg en medarbejder, som er ansvarlig for administration af virksomhedens brugerrettigheder. Medarbejderen skal oprette brugeradgange, når nye medarbejdere starter. Ændre brugeradgange, hvis en medarbejder fx får nyt ansvarsområde. Og slette brugeradgange, når medarbejdere stopper.

Hvis jeres IT-leverandør håndterer styring af jeres brugeradgange, er det vigtigt, at I stiller krav til deres håndtering og kvalitetssikring af brugerstyringen.

Sikring af fjernadgang (remote acces)

I mange virksomheder har medarbejdere mulighed for at arbejde hjemmefra, eller når de er på farten. Her bør ledelsen overveje, hvordan medarbejdere, der arbejder via *remote acces,* kan få adgang til virksomhedens systemer og data på en sikker måde.

Den tekniske løsning kan være at opsætte en lukket, krypteret forbindelse (Virtual Private Network, VPN) mellem virksomhedens systemer og medarbejdernes computere, tablets eller mobiltelefoner.

Den organisatoriske løsning kan være en regel om, at medarbejdere ikke må behandle følsomme data som eksempelvis personoplysninger eller forretningshemmeligheder, når de bruger *remote access.*

Stil krav til sikkerheden i medarbejdernes adgangskoder

Sikre passwords gør det sværere at få adgang for IT-kriminelle. Et sikkert password skal:

1) Være langt – dvs. mindst 10 tegn.

2) Være nyt – dvs. skiftes ud ofte.

3) Være varieret – dvs. indeholde store og små bogstaver, tal og specialtegn.

For de mest kritiske systemer og de systemer med jeres vigtigste data, kan I overveje at implementere multi-faktor login.

Se flere gode råd om bl.a. passwords på SikkerDigital.

Se også Center for Cybersikkerheds passwordguide

Insidertruslen

IT-kriminelle går ofte efter medarbejdere for at få adgang til systemer og data. Det er som regel på grund af uvidenhed eller uforsigtighed, at medarbejdere udgør en risiko for deres arbejdsplads. Der er dog i visse tilfælde medarbejdere, der helt bevidst går efter at misbruge deres adgang til virksomhedens systemer eller data. Det kan være for egen vindings skyld, fordi den pågældende medarbejder føler sig dårligt behandlet eller på grund af noget helt tredje.

Derfor bør jeres virksomhed tage stilling til, hvordan I bedst forhindrer, at nuværende og tidligere medarbejdere forvolder skade på data eller systemer.

Anbefaling til, hvordan I beskytter jeres virksomhed mod insidere

- Begræns adgang til systemer og data for medarbejdere.
- Hav en fast procedure ved opsigelser.
- Log brugeraktivitet i jeres systemer.

Begræns adgang til data og systemer

Ved at styre medarbejderes adgangsrettigheder kan virksomheden sikre, at hver enkelt medarbejder kun har adgang til de data og systemer, som er nødvendige for at vedkommende kan udføre sit arbejde. Når færre medarbejdere har adgang til de mest kritiske systemer og data nedbringes sandsynligheden for, at en nuværende eller tidligere medarbejder kan misbruge sin adgang til at skade virksomheden.

Læs også Anbefaling 8 – styring af medarbejdernes adgang til jeres informationer og systemer.

En af mulighederne for at begrænse medarbejderes adgang kan være gennem separation af rettigheder. Det betyder, at en enkelt medarbejder ikke på egen hånd kan udføre bestemte handlinger fx overføre større pengebeløb eller slette vigtige filer.

Hav en fast procedure ved opsigelser

En opsagt medarbejder kan beslutte sig for at stjæle fortrolige oplysninger eller slette vigtige data, hvis vedkommende føler sig dårligt behandlet. Derfor bør jeres virksomhed have en fast procedure ved opsigelse af medarbejdere, som tager højde for risikoen for, at den opsagte medarbejder kan have til hensigt at skade virksomheden.

Log brugeraktivitet i jeres systemer

Der kan være filer eller systemer, som det er nødvendigt, alle medarbejdere har adgang til. Men som det vil have store konsekvenser, hvis en medarbejder sletter eller ødelægger. Somme tider er det muligt at stoppe vedkommende, hvis I har et program, der registrerer jeres logfiler i realtid. Programmet kan sende advarsler, når der er aktivitet, som falder udenfor det normale. For at sikre, at logningen virker, kan det være en god ide at sikre, at ingen medarbejdere på egen hånd kan slette logfilerne. Det kan fx gøres ved at gemme logfilerne to forskellige steder (redundant logning). Implementering af redundant logning kan være temmelig vanskeligt og skal muligvis gøres i samarbejde med en IT-leverandør eller rådgiver.

Læs også Anbefaling 15 – Overvågning og logning af virksomhedens IT-systemer

Styrk medarbejdernes IT-sikkerhedsviden

Mange sikkerhedsbrud sker på grund af fejl og manglende viden blandt medarbejdere. De kan fx blive narret til at klikke på et usikkert link eller udlevere deres adgangskode. Derfor er det afgørende for virksomhedens IT-sikkerhed, at medarbejdere lærer, hvordan kan reducere risikoen for, at virksomheden bliver ramt af fx et hackerangreb eller en computervirus.

Anbefalinger til styrket IT-sikkerhedsviden hos medarbejderne

- Kommuniker de vigtigste budskaber om IT-sikkerhed til medarbejderne.
- Kommuniker IT-sikkerhed på flere forskellige måder.
- Sørg for løbende at opdatere medarbejderes viden om god IT-sikkerhed.

Kommuniker de vigtigste budskaber om IT-sikkerhed til medarbejderne

Hvilke IT-sikkerhedsemner, I vil kommunikere til jeres medarbejdere, afhænger af jeres medarbejdere og virksomhedens risikoprofil. I kan fx starte med at kigge på følgende:

- Opmærksomhed og sund skepsis overfor mails fra fremmede – fx mails med et link til en mistænkelig hjemmeside eller vedhæftede dokumenter, som kan være inficeret med virus.
- Betydningen af stærke adgangskoder - et godt password skiftes ofte, er langt og vanskeligt for hackere at gætte.
- Fokus på ikke at dele personfølsomme oplysninger og andre fortrolige oplysninger digitalt.
- Viden og læring om, hvordan medarbejderne skal reagere, hvis deres computer bliver inficeret med et virusangreb.

Se meget mere på Erhvervsstyrelsens kampagneside Klik ikke her. Kampagnen sætter fokus på at styrke en sikker it-adfærd blandt medarbejdere. Her kan virksomheder downloade enkle og iøjnefaldende kommunikationsmaterialer, blandt andet print-selv plakater med de tre gode råd, en PDF-præsentation samt sjove print-selv plakater til kantinen, kopirummet osv.

Kommuniker IT-sikkerhed på flere forskellige måder

Kommunikation om IT-sikkerhed kan ikke klares én gang på ét morgenmøde.

Der er mange måder at få give jeres budskaber videre til medarbejderne på. Ofte vil en kombination af flere måder være mest effektiv og påvirke flest mulige medarbejdernes adfærd i den rigtige retning. I kan fx:

- afholde medarbejdermøder, hvor I mundtligt kommunikerer jeres IT-sikkerheds-retningslinjer kombineret med gode IT-sikkerhedsråd.
- sørge for at nye medarbejdere som en del af deres velkomst også får relevant viden om virksomhedens IT-sikkerhed.
- præsentere jeres gode IT-sikkerhedsråd på plakater rundt omkring i bygningen.
- vælge at købe vejledning til en oplysnings- og uddannelseskampagne hos en ekstern leverandør.

Løbende opdatering af medarbejderes viden om god IT-sikkerhed

IT-kriminelle ændrer konstant metoder og finder nye måder at svindle eller narre virksomheders medarbejdere på. Det er vigtigt, at I overvejer om nye emner skal kommunikeres og medarbejdernes viden skal genopfriskes. Vurder gerne dette halvårligt.

Beskyt virksomhedens datanetværk

Virksomheder har ofte et internt netværk, der forbinder computere, printere og anden hardware, ligesom der ofte er et eksternt netværk, som giver adgang til internettet. Hackere kan angribe både interne og eksterne netværk, som derfor bør beskyttes.

Invester i en sikkerhedspakke

For at sikre tilgangen til jeres datanetværk og samtidig begrænse uvedkommendes adgang til jeres systemer bør I investere i en sikkerhedspakke, som indeholder de mest almindelige sikkerhedsmoduler. Som minimum bør pakken indeholde:

- Antivirus
- Firewall
- Antispyware
- Sårbarhedsscanner
- Spamfilter
- Antiphishing

Lav regler for tilkobling af medarbejdernes private enheder på virksomhedens netværk

Mange steder er det almindeligt, at medarbejdere tilkobler deres egne enheder (*devices)* på virksomhedens netværk – fx logger på firmaets WiFi med deres private smartphone. Det medfører en risiko for at skadelig software finder vej ind i virksomhedens systemer. Derfor kan det være en god ide at lave et sæt regler for BYOD (dvs. *Bring Your Own Device*).

Sikring af fjernadgang (remote acces)

I mange virksomheder har medarbejdere mulighed for at arbejde hjemmefra, eller når de er på farten. Her bør ledelsen overveje, hvordan medarbejdere, der arbejder via *remote acces,* kan få adgang til virksomhedens systemer og data på en sikker måde.

Den tekniske løsning kan være at opsætte en lukket, krypteret forbindelse (Virtual Private Network, VPN) mellem virksomhedens systemer og medarbejdernes computere, tablets eller mobiltelefoner.

Den organisatoriske løsning kan være en regel om, at medarbejdere ikke må behandle følsomme data som eksempelvis personoplysninger eller forretningshemmeligheder, når de bruger *remote access.*

Incident Prevention System (IPS) & Incident Detection System (IDS)

For virksomheder, der har brug for at have et mere avanceret IT-sikkerhedsniveau, kan det overvejes at supplere sikkerhedspakken med IPS og/eller IDS. De er ret sofistikerede løsninger, men kort fortalt er:

- IPS en løsning som forhindrer adgang til netværket. På den måde minder en IPS om en firewall, men IPS'en er mere grundig og kigger på flere aspekter af den indgående netværkstrafik.
- IDS-teknologi fortæller dig om trafikken ind på dit netværk. Det er en måde at overvåge den indgående netværkstrafik, så det er muligt at holde øje med, om der er potentielle trusler, som skal undersøges nærmere.

Anbefaling 12 - Opdatering af it-systemer

Hold IT-systemer opdaterede

Hackere opdager hele tiden nye sårbarheder i computerprogrammer og -styresystemer, som kan udnyttes til at få adgang til data og netværk. Ved at opdatere programmer kan man lukke mange af disse "huller" i sikkerheden.

Løbende opdateringer af jeres systemer kan ligeledes hjælpe jer i en situation, hvor I skal have hjælp til et system fra den pågældende IT-leverandør, da leverandører ofte ikke yder support på meget forældede og ikke-opdaterede versioner af systemerne.

I bør som udgangspunkt opdatere alle systemer, herunder firewalls, antivirus, og alle programmer på medarbejdernes computere, så snart leverandørerne frigiver nye opdateringer.

Anbefalinger til opdatering af IT-systemer

- Slå automatisk sikkerhedsopdatering til
- Opdater ofte
- Udpeg en ansvarlig

Slå automatisk sikkerhedsopdatering til

Mange programmer kan indstilles til automatisk at blive opdatere, når en ny version er tilgængelig. Slå automatisk opdatering til, hvor det kan lade sig gøre – på den måde er der færre programmer, I selv skal holde øje med.

Hvis I har programmer eller systemer, som af den ene eller den anden grund ikke kan opdateres, bør I overveje at erstatte det med en nyere version. I kan også overveje at isolere enkelte programmer, så der ikke kan kommunikeres til det fra netværket. Dette kræver dog en del ressourcer, så det vil ofte være nemmere at skifte til en løsning, som det er muligt at opdatere.

Opdater ofte

I bør opdatere jeres programmer og systemer regelmæssigt – fx en gang om måneden.

For nogle systemer er det et krav, at jeres virksomhed håndterer opdateringen af sårbarhederne. Spørg evt. jeres leverandør, hvad kravene til jeres systemer er.

Det kan være en fordel at undersøge, hvor ofte leverandørerne udgiver opdateringer til jeres programmer og systemer. Microsoft (Windows, Office mv.) udgiver fx nye opdateringer en gang om måneden. For andre systemer kan der være kvartalsvise eller løbende opdateringer.

Husk at sikre, at der er taget backup, inden opdateringen går i gang, så systemet kan rulles tilbage i tilfælde af, at opdateringen ikke går efter hensigten.

Udpeg en ansvarlig

Opdatering af systemer er en vigtig del i jeres IT-sikkerhedsarbejde, derfor bør I udpege en eller flere person, som har ansvaret for, at alle systemer bliver opdateret.

Hvis jeres it-leverandør står for opdatering af jeres systemer og programmer, bør I stille krav til deres håndtering af opdateringer som en del af jeres leverandøraftale.

Se også Anbefaling 16 – IT-sikkerhed hos jeres samarbejdspartnere

Beskyt virksomheden mod virus og andre typer malware

Malware er en samlebetegnelse for ondsindet software, som har til formål at skade virksomhedens programmer og data. Malware kan gøre stor skade på kort tid, hvis ikke man er påpasselig. Det ondsindede software kan fx slette jeres data eller stjæle informationer. En af de mest kendte og udbredte typer malware er virusangreb. Mange virksomheder er blevet ramt af virusangreb, ofte med meget skadelige konsekvenser til følge.

Anbefalinger til at beskytte jeres virksomhed mod malware

- Installer en sikkerhedspakke
- Uddan jeres medarbejdere i sikker digital adfærd
- Reager hurtigt på malwareangreb

Installer en sikkerhedspakke

For at kunne beskytte jeres virksomhed mod malware og virusangreb er det helt grundlæggende, at I har installeret antivirusprogrammer på alle virksomhedens computere og servere.

I bør overveje, hvilke øvrige enheder der skal beskyttes imod virusangreb. Det kan fx være computere, som er offentligt tilgængelige eller delt mellem flere medarbejdere (fx en delt pc på et værksted eller i en butik). Bruger I smartphones, bør I ligeledes overveje at beskytte disse med antivirusprogrammer. Som minimum bør pakken indeholde:

- Antivirus
- Firewall
- Antispyware
- Sårbarhedsscanner
- Spamfilter
- Antiphishing

Når I investerer i et antivirusprogram, er det vigtigt at kontrollere, om antivirusprogrammet er aktivt hele tiden, samt at antivirusprogrammet automatisk opdateres, minimum hver dag. Læs grundigt specifikationerne for produktet for at sikre dette.

Uddan jeres medarbejdere i god IT-adfærd på nettet

Langt de fleste virusangreb skyldes medarbejdernes manglende viden og utilsigtede fejl på internettet. Mange af de virusangreb, der eksisterer i dag, er desværre designet specifikt til at omgå antivirusprogrammer.

Det er derfor vigtigt, at jeres medarbejdere er bevidste om, hvordan de bedst muligt undgår at blive inficeret med malware og virus. Se mere i Anbefaling 10 – Styrkelse af medarbejdernes IT-sikkerhedsviden.

Reager hurtigt på angreb

Hvis jeres virksomhed bliver ramt af et virusangreb, er det vigtigt, at medarbejderne ved, hvordan de hurtigt og effektivt skal reagere. Skaden kan blive meget større, hvis virusangreb ikke håndteres korrekt og hurtigt bremses.

Det er vigtigt, at jeres medarbejdere er klar over, at de straks skal frakoble den virusinficerede maskine fra netværket og derefter hurtigst muligt udfører en fuld antivirusscanning (evt. med hjælp fra den it-sikkerhedsansvarlige i virksomheden)

Det kan ofte være svært at komme helt af med virus, hvis man først er inficeret og ofte vil det være sikrest at genetablere hele computeren.

Det kan være en god ide at søge hjælp fra IT-eksperter, hvis først uheldet er ude for derved at sikre at de IT-kriminelle ikke har installeret ”bagdøre”, som de efterfølgende kan bruge.

Håndteringen af en it-sikkerhedshændelse handler både om at minimere skaden og stoppe angrebet. Men det handler også om at sikre, at du har beviser der kan være med til at identificere den it-kriminelle.

Læs meget mere om, hvad du gør hvis virksomheden er blevet ramt på SikkerDigital.

Effektiv backup

En af de mest almindelige årsager til, at virksomheder mister deres data, er ingen eller mangelfuld backup. Mister virksomheden sine data er det besværligt, frustrerende og kan have store økonomiske konsekvenser. Årsagerne til datatab er mange. Virksomhedens IT-udstyr kan blive udsat for brand eller vandskade. Eller data kan blive stjålet eller krypteret som følge af angreb fra IT-kriminelle. Skulle virksomheden blive udsat for systemnedbrud, brand, virusudbrud eller andet datatab, er det afgørende, at vigtige informationer løbende bliver gemt og kan genskabes. For at beskytte virksomhedens data er det nødvendigt at begrænse medarbejdernes adgang, så medarbejderne kun har adgang til data, som er påkrævet i opgaveløsningen. Sikre og enkle backuprutiner er derfor afgørende, hvis I løbende vil sikre virksomheden mod tab af værdifulde og forretningskritiske data.

Fire trin til backup af din virksomheds data

1

Hvad skal sikkerhedskopieres?

- Identificer hvilke typer data jeres virksomhed har brug for at tage backup af.
- Det kan fx være forretningskritiske data som kundeinformation, forretningshemmeligheder, finansielle oplysninger osv.

2

Tag backup ofte og udpeg en ansvarlig

- Sørg for at tage backup jævnligt, gerne ugentligt eller dagligt.
- Sørg for at udpege en ansvarlig medarbejder for backupprocesser i virksomheden – det kan fx være den IT-ansvarlige eller virksomhedsejeren selv.

3

Opbevar virksomhedens backup sikkert

- Backup af dine data kan fx lagres i internetbaserede cloud-løsninger, på eksterne drev eller andre medier.
- Det er vigtigt, at virksomhedens backup lagres et andet sted end i virksomheden i tilfælde af brand eller vandskade.
- Overvej også om data skal krypteres. Kryptering af data sikrer, at uvedkommende ikke har mulighed for at aflæse dine data. Husk persondata skal altid krypteres!
- Beslut, hvor længe backup skal gemmes.

4

Test at den virker

- Mange virksomheder opdager først, når skaden er sket, at deres backup ikke fungerer efter hensigten.
- Tjek derfor, at jeres backup fungerer og at data kan læses tilbage til systemerne.
- Hvis jeres IT-leverandør håndterer jeres backup, er det vigtigt, at I stiller krav til deres håndtering og kvalitetssikring af backupprocessen.

Logning af de vigtigste IT-systemer

Logning, dvs. registreringer af aktiviteter i virksomhedens IT-systemer er et vigtigt redskab for at opdage hvis noget går galt fx hvis I mister data efter angreb af IT-kriminelle. Samtidig er det vigtigt at kunne sikre beviser til efterforskning og målrette, hvor I skal sikre systemerne bedre. For ikke at bruge unødige ressourcer på logning af virksomhedens systemer, anbefales det at prioritere de systemer, som opbevarer eller behandler forretningshemmeligheder og/eller følsomme personoplysninger.

Overvågning af logs, kræver dog ofte specialistviden, fx for at kunne identificere nye typer af hackerangreb. I kan derfor overveje, om jeres logovervågning skal håndteres af en ekstern leverandør.

Anbefalinger til overvågning af de vigtigste systemer i virksomheden

- Giv medarbejderne besked om overvågning af systemer
- Prioriter hvilke systemer I vil overvåge
- Beslut hvor ofte I gennemgår jeres logs og hvordan I gemmer dem

Giv medarbejderne besked om overvågning af systemer

Inden I begynder at overvåge de vigtigste systemer i virksomheden, skal I være opmærksomme på, at medarbejderne, der benytter disse systemer, skal informeres om det.

Medarbejderne skal på forhånd være klart informeret om, at registreringen/logningen finder sted, og at registreringen eventuelt vil blive gennemset som led i en kontrol ved mistanke om uregelmæssigheder i vitale IT-systemer.

Prioriter hvilke systemer i vil overvåge

I skal starte med at bestemme, hvilke systemer I har brug for at overvåge og logge.

I bør primært logge systemer med forretningshemmeligheder og følsomme personoplysninger - gerne på baggrund af jeres risikovurdering. Se Anbefaling 3 om risikovurdering.

Det anbefales, at I overvejer logning af følgende:

- IT-sikkerhedsløsninger: Fx Firewall, antivirus m.m.
- Fx Mail exchange-server, webservere, Virtual Private Network (VPN) mm.
- Systemer med forretningshemmeligheder og følsomme personoplysninger.

Beslut hvor ofte I gennemgår jeres logs og hvordan I gemmer dem

Når I har besluttet, hvad I vil logge, skal I tage stilling til følgende:

- Hvor tit vil gennemgå jeres logning? (fx regelmæssigt eller ved en konkret sikkerhedshændelse)
- Hvor lang tid vil I opbevare de enkelte logs?
- Vil I bruge et overvågningssystem, kaldet et SIEM-værktøj (Security Information & Event Management)? Systemet giver mulighed for at kunne identificere mønstre og sammenhænge på tværs af systemerne og samler alle logs i ét system.
- Hvis I fravælger SIEM-værktøjet bør I selv lagre jeres logs sikkert og centralt
- Hvor lang tid vil I opbevare de enkelte logs?

I mange tilfælde er der gået uger eller måneder, fra et hackerangreb er udført og til virksomheden har opdaget hændelsen. I en sådan situation er det vigtigt, at de relevante logs ikke er blevet slettet.

I bør opbevare de enkelte logs i så lang tid, som det giver mening for jeres virksomhed. I kan med fordel bruge disse guidelines til opbevaringsperiode i forhold til betydning:

- Aktiviteter der logges har *lav* betydning: Opbevaring i 1-2 uger
- Aktiviteter der logges har *medium* betydning: Opbevaring i 1-3 måneder

- Aktiviteter der logges har *høj* betydning: Opbevaring i 3-12 måneder

HUSK: Logning kræver plads og vedligeholdelse i jeres IT-systemer. I skal have overblik over hvordan logs opbevares og hvem der har adgang til at læse, ændre og slette dem.

Yderligere information

Læs logningsvejledning fra Center fra Cybersikkerhed.

IT-sikkerhed hos jeres samarbejdspartnere

Mange danske virksomheder vælger at outsource hele eller dele af deres IT-drift til eksterne IT-leverandører. Det er dog altid virksomhedens eget ansvar, at IT-sikkerheden er i orden. Det er derfor afgørende at få stillet de rigtige spørgsmål og sikkerhedskrav til jeres samarbejdspartner og få det skrevet ind i jeres samarbejdskontrakt. Når kravene er på plads, skal virksomheden og leverandør aftale, hvem der har ansvaret for hvad.

Her er anbefalinger til spørgsmål og sikkerhedskrav, I kan stille til jeres IT-leverandør for at sikre jeres It-sikkerhed og data bedst muligt:

Stil krav til leverandørens opbevaring af jeres data ved at spørge:

- Hvor ligger virksomhedens data rent fysisk? Dvs. hvilken lokation og i hvilket land står serverne, der indeholder jeres virksomhedsdata?

Stil krav til leverandørens IT-processer ved at spørge:

- Hvordan og hvor tages backup?
- Hvad er processen for antivirusprogrammer og deres opdatering?
- Hvordan er processen for opdateringer og ændringer af IT-systemer programmer?
- Hvordan styrer I brugeradgang og -rettigheder til IT-systemerne?

Stil krav til leverandørens IT-sikkerhedsforanstaltninger ved at spørge:

- Hvordan sikrer I sikkerheden mellem datanetværkerne? Fx via logning af netværker, segmentering af netværker, firewall etc.?
- Hvordan dokumenterer I virksomhedens netværker. Fx i en grafisk netværksoversigt.

Stil krav til IT-leverandørens beredskab og test af sikkerhedsløsninger ved at spørge:

- Har I en IT-beredskabsplan? Det skal fx fremgå, at leverandøren giver virksomheden besked ved sikkerhedshændelser)
- Tester i løbende IT-sikkerheden i virksomheden?

Stil krav til leverandørens behandling af persondata ved at spørge:

- Hvordan håndterer I persondata?
- Hvordan sikrer i fortroligheden af de persondata, I behandler for os?

Vær opmærksom på: Hvis jeres IT-leverandør håndterer persondata, stiller GDPR ekstra krav. Så skal I aftale, hvem der er dataansvarlig og databehandler for hvilke behandlinger. I skal eventuelt indgå en data-behandleraftale eller en aftale om fordelingen af ansvaret mellem to dataansvarlige.

Læs mere om databehandleraftaler i Anbefaling 17 – Lav en databehandleraftale.

Stil krav til leverandørens løbende afrapportering

Leverandøren skal løbende rapportere (fx kvartalsvist) om sikkerhedshændelser og status på de sikkerhedsprocedurer, som er aftalt i samarbejdskontrakten. På den måde får I indsigt i, om leverandøren lever op til sine forpligtelser og om jeres IT-sikkerhedsniveau er i orden.

Hvis jeres leverandør udvikler softwarekode for jeres virksomhed, er det vigtigt, at I får afklaret, hvem der beholder de immaterielle rettigheder. I skal sørge for at have en kopi af konfigurationsfiler og kildekode i tilfælde af, at I ønsker at skifte leverandør.

Anbefaling 17 – Lav en databehandleraftale

Lav en databehandleraftale

Hvis jeres virksomhed har bedt andre om at behandle personoplysninger på virksomhedens vegne, skal der være en skriftlig databehandleraftale på plads ifølge databeskyttelsesforordningen (GDPR). Det er jeres virksomhed, som har ansvaret for, at oplysningerne opbevares og behandles korrekt. Aftalen skal derfor nøje beskrive, hvordan samarbejdspartneren skal sikre dine data.

Anbefalinger til at lave en databehandleraftale

- Afklar jeres rolle
- Forstå og implementer kravene til en databehandleraftale

Afklar jeres rolle

I skal være opmærksomme på, hvilken rolle I spiller i forbindelse med databehandling. Om I er dataansvarlig, databehandler eller deler dataansvaret har betydning for, hvilke krav I skal leve op til.

Se mere om, hvordan I kan afklare jeres rolle som enten dataansvarlig eller databehandler.

Forstå og implementer kravene til en databehandleraftale

Databehandleraftalen skal være en skriftlig aftale mellem jeres virksomhed og jeres leverandør.

En databehandleraftale skal indeholde**:**

- Rammen for behandling af personoplysninger
- Dokumenteret instruks
- Fortrolighed og tavshedsforpligtelse
- Tekniske og organisatoriske sikkerhedsforanstaltninger
- Bistand til den dataansvarlige
- Underretning om brud på sikkerheden
- Underdatabehandlere
- Eventuelt en fortegnelse over behandlingsaktiviteter
- Revision af efterlevelse af aftalen
- Eventuel overførsel til tredjeland
- Sletning eller tilbagelevering af personoplysninger
- Underretning om ulovlig instruks

Jeres databehandleraftale er et vigtigt og lovpligtigt dokument. I bør derfor vurdere, om I selv kan udforme aftalegrundlaget, eller om I har behov for at søge ekstern hjælp.

Læs mere om kravene til en databehandleraftale.

Yderligere information

Se Datatilsynets skabelon for at lave en databehandleraftale.