Rapport

Anbefaling

God IT-sikkerhed er god forretning. En brist i jeres IT-sikkerhed kan koste din virksomhed mange penge i genopretning af dine systemer, data og ikke mindst dit omdømme hos dine kunder og samarbejdspartnere.

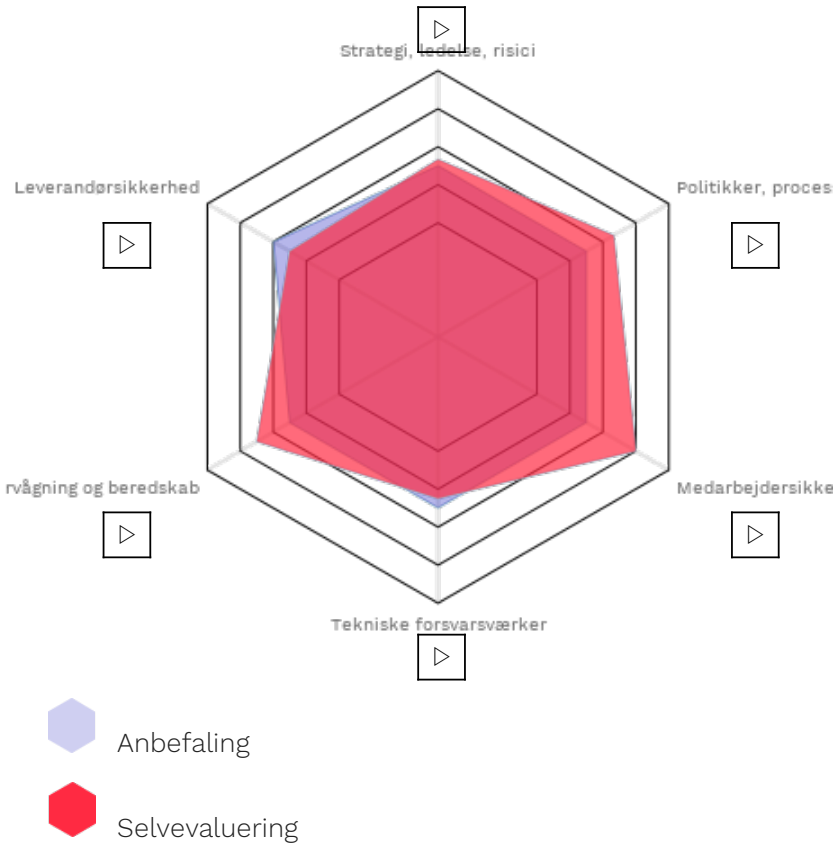
I spindet til højre kan du se din virksomheds aktuelle sikkerhedsniveau (det grå felt) holdt op mod det anbefalede for netop din virksomhed (det røde felt), som er skabt ud fra besvarelserne af, om jeres virksomhedsstørrelse, branche, om I har kritiske systemer og personfølsomme data samt graden af outsourcing. Spindet skal give et fingerpeg af, hvor fokus bør være i jeres fremadrettede sikkerhedsindsats.

I bør overveje, at styrke jeres IT-sikkerhed på områder, hvor jeres aktuelle niveau ligger under det anbefalede. Nedenfor finder I vejledning til, hvordan I kan gribe det an på de 3 områder, hvor jeres svar indikerer det største behov for handling.

Se også, hvad der sker, når en virksomhed oplever et sikkerhedsbrud, og hvordan man kan forebygge at det sker. Videoerne finder I under de 6 temaer i spindet.

Hvis du ønsker at se, hvad du har svaret på spørgsmålene, kan du klikke tilbage i tjekket. Du kan også se og printe en pdf-rapport over dine svar og det anbefalede niveau på de enkelte spørgsmål samt vejledning til, hvordan I kan styrke virksomhedens it-sikkerhed.

Og husk: Trusselsbilledet ændrer sig hele tiden, og det gør din virksomhed sikkert også. Jeres IT-sikkerhed bør derfor løbende tages op til revision. Genbesøg derfor sikkerhedstjekket regelmæssigt og se om jeres IT-sikkerhed er up-to-date.



Sådan kommer du igang

Du bør læse:

Kapitel 18
Kapitel 6
Kapitel 1

HENT RAPPORT SOM PDF

Spørgsmål	Svar	Anbefalet	Læs mere
1. Har virksomhedens ledelse taget stilling til hvordan it-sikkerhed bedst håndteres i virksomheden?	1	3	Kapitel 1
2. Er kritiske informationer og systemer identificeret?	4	3	Kapitel 2
3. Kender vi de sikkerhedstrusler vores forretning står over for og hvordan disse kan påvirke vores forretning?	3	3	Kapitel 3
			Kapitel

4. Har virksomheden dokumenteret arbejdet med it-sikkerhed?	5	3	Kapitel 4
5. Hvordan sikrer vi, at følsomme persondata håndteres på sikker vis?	4	3	Kapitel 5
6. Hvordan sikres det, at ændringer af systemer og programmer sker på sikker vis?	0	3	Kapitel 6
7. Hvordan styrer virksomheden medarbejdernes adgang til informationer og systemer?	3	3	Kapitel 7
8. Har virksomheden fået foretaget en uafhængig gennemgang af informationssikkerheden?	5	3	Kapitel 8
9. Har virksomheden en effektiv backup-proces i tilfælde af systemsammenbrud eller datatab?	3	3	Kapitel 9
10. Hvordan sikres det, at medarbejderne er bevidste om informationssikkerhed?	4	3.5	Kapitel 10
11. Hvordan beskyttes virksomhedens interne og eksterne data-netværk?	2	3.5	Kapitel 11
12. Hvordan sikres det, at virksomhedens it-programmer og systemer holdes sikkerhedsmæssigt opdateret?	3	3.5	Kapitel 12
13. Hvordan beskytter virksomheden sine arbejdssituationer og servere mod malware?	2	3.5	Kapitel 13
14. Hvordan sikres den fysiske adgang til virksomhedens kritiske informationer?	2	3.5	Kapitel 14
15. Har virksomheden en effektiv plan for at opdage og håndtere brud på sikkerheden?	5	3.5	Kapitel 15
16. Foretages der overvågning af sikkerheden i virksomhedens it-systemer?	2	3.5	Kapitel 16
17. Er sikkerhedsaspekterne i relationen til virksomhedens samarbejdspartnere identificeret?	4	4	Kapitel 17
18. Har virksomheden udformet en databehandleraftale, der beskriver, hvordan leverandørerne skal håndtere personfølsomme informationer?	1	4	Kapitel 18

Kapitel 1

LEDELSENS INVOLVERING, HÅNDTERING OG ANSVAR I FORHOLD TIL JERES VIRKSOMHEDS IT-SIKKERHED

Hvorfor er det vigtigt, at ledelsen forholder sig til virksomhedens it-sikkerhed?

I dag er stort set alle virksomheder konstant online, hvilket markant øger virksomhedens risiko for at blive ramt af it-kriminalitet og andre it-sikkerhedshændelser.

It-kriminalitet rammer alle organisationer, uafhængig af størrelse, type eller branche.

Ledelsen skal sikre, at der er en sammenhæng mellem den type forretning, som I driver, jeres risikoprofil og jeres valgte sikkerhedsforanstaltninger.

Håndteringen af jeres virksomheds it-sikkerhed er et løbende arbejde, som bør integreres i det samlede ledelsesarbejde og styring af virksomheden. It-sikkerhed er ledelsens ansvar på lige fod med økonomi, arbejdsmiljø, kundeservice osv.

Derfor bør jeres virksomheds ledelse være direkte involveret i fastlæggelsen af et tilstrækkeligt sikkerhedsniveau og i handlinger og kommunikation signaler, at it-sikkerheden er prioriteret i jeres virksomhed.

Anbefalinger til, hvad ledelsen skal tage stilling til

- Forstå og beskriv jeres risikovillighed, dvs. hvilken risiko ledelsen villig til at acceptere for at kunne drive virksomhedens kerneforretning.
- Ledelsen skal påtage sig et ansvar og optræde som rollemodel i forhold til virksomhedens arbejde med it-sikkerhed.
- Ledelsen skal sikre en løbende styring af virksomhedens it-sikkerhedsarbejde.

Forstå og beskriv jeres risikovillighed

Fastlæggelse af jeres risikovillighed ligger oftest forud for en risikovurdering, hvor ledelsen vurderer, hvilken risiko I er villige til at acceptere for at kunne drive jeres kerneforretning.

For at få et overblik over jeres virksomheds risikovillighed anbefales det, at I starter med at identificere, hvilke systemer, processer og data som

er mest kritiske for jeres virksomhed. Se vejledning om kritiske data og systemer på ww.sikkerhedstjekket.dk.

I bør ligeledes forstå, hvilke motiver de it-kriminelle har for at ramme jeres virksomhed. Er det fx målrettet spionage eller vilkårlig it-kriminalitet med økonomisk afpresning, som er mest sandsynlig for jeres virksomhed?

I bør overveje, om jeres virksomhed selv har den fornødne viden til at fastlægge jeres risikovillighed og udarbejde en risikoanalyse for jeres virksomhed, eller om I bør søge ekstern sparring.

Ledelsen skal optræde ansvarligt og som rollemodel

Lederne bør i kraft af deres adfærd vise medarbejderne, hvor vigtigt det er for jeres virksomhed at passe godt på organisationens informationer.

Ledelsen bør således gå forrest og være med til at skabe en sikkerhedskultur, som matcher jeres virksomheds behov. Ledelsen bør tage ansvar for, at virksomhedens sikkerhedskultur bliver en integreret del af virksomheden.

For at skabe en god sikkerhedskultur bør ledelsen indføre små, men meningsfulde aktiviteter i hverdagen, som matcher virksomhedens forretningsgrundlag. De små daglige aktiviteter skal primært styrke medarbejdernes opmærksomhed på beskyttelse af virksomhedens opbevaring af kundeoplysninger og andre fortrolige informationer. På et kontor, kan en aktivitet være, at medarbejderne ikke må gå fra deres computer, med mindre de låser skærmen, for at undgå, at uvedkommende kan få adgang til computeren. På en byggeplads, hvor mobile devices kan være en væsentlig informationskilde, bør medarbejderne have et stærkt password på de mobile devices.

At sikre en løbende håndtering af jeres it-sikkerhedsarbejde

Arbejdet med jeres virksomheds it-sikkerhed er en løbende proces, fra forståelse af krav og behov i relation til jeres it-sikkerhedsniveau og til implementering af sikkerhedsforanstaltninger og opfølgning.

Sikkerhedsarbejde

Trusselbilledet ændrer sig konstant; derfor det er vigtigt, at I løbende forholder jer til, hvilke sikkerhedsforanstaltninger jeres virksomhed har brug for. God praktik er mindst én gang om året at revurdere jeres behov og krav til virksomhedens it-sikkerhedsniveau.

Hvorfor er det vigtigt at have en proces for håndtering af ændringer i jeres it-systemer?

It-systemer skal løbende ændres og opdateres. Når man udfører ændringer i it-systemer og software, sker det ofte, at man kommer til at lave sikkerhedshuller, hvis ikke ændringerne er nøje styret.

Manglende styring af processen for håndtering af ændringer kan således føre til fejl i systemerne og dermed medføre, at medarbejderne ikke kan få adgang til det pågældende system i en kortere eller længere periode, at virksomheden kan miste data, og at genetableringsprocessen kan være lang og vanskelig.

En proces for håndtering af ændringer i jeres it-systemer, it-programmer og it-produktionsapparat skal kvalitetssikre jer mod sådanne situationer.

Anbefalinger til håndtering af ændringer i it-systemer

- I skal udarbejde retningslinjer for ændringer i jeres it-systemer – både hvis I selv foretager ændringerne, eller hvis de bliver udført af jeres it-leverandør.
- I skal sørge for at have den rigtige bemanding og evt. support fra jeres it-leverandør, når I foretager ændringerne.
- I skal stille krav til, hvordan jeres it-leverandør håndterer ændringerne i jeres systemer.

Udarbejdelse af retningslinjer for ændringer i jeres it-systemer

Hvis I selv håndterer ændringerne i jeres systemer, bør I have en ensartet, afstemt og evt. nedskrevet håndtering af, hvordan, hvornår og af hvem ændringerne skal foretages. Samme retningslinjer bør gælde for jeres it-leverandør.

I skal overveje, hvilke elementer der er nødvendige ved implementering af en ændringen. Dette kan fx være:

- Kategorisering : Er det en mindre og ikke kompleks ændring eller en større opdatering?

- Prioritering : Hvor meget haster ændringen, og er der forhold, som kræver, at den implementeres (fx lovgivning, der skal overholdes)?

- Implementeringsplan : Trinvis plan inkl. vurdering af tidsforbrug med de handlinger, som skal gennemføres i forbindelse med ændringen.

- Roll-back plan : Trinvis plan inkl. tidsforbrug for, hvordan den tidligere tilstand kan genetableres i tilfælde af, at ændringen mislykkes.

- Resultat af test : Hvis ændringen er testet, eksempelvis i et testmiljø, bør testresultaterne i tilfælde af gode erfaringer implementeres i processen.

Sikring af rigtig bemanding ved ændringer i jeres it-systemer

I bør beslutte og gerne skriftlig dokumentere, hvilken medarbejder der har ansvaret for ændringen, og om I har behov for andre støttende kompetencer undervejs i forløbet.

I bør vurdere, om ændringen skal godkendes af en leder, og på hvilket niveau.

Såfremt I selv foretager ændringerne, bør I vurdere, om der er behov for en permanent ordning eller en tilkaldeordning under/efter implementering af ændringen med jeres it-leverandør, hvilket bør defineres i jeres kontrakt med leverandøren.

Hvis jeres it-leverandør varetager ændringer i jeres systemer, bør I stille krav til deres kvalitetssikring i henhold til proces og bemanding.

Hvorfor er det vigtigt at have en databehandler-aftale?

En databehandleraftale er en skriftlig aftale mellem jeres virksomhed og jeres it-driftsleverandør om opbevaring og behandling af jeres persondata.

Når jeres virksomhed overlader opbevaring og behandling af personoplysninger til en anden virksomhed, er det et lovkrav i henhold til persondataloven, at der indgås en databehandleraftale.

Persondataloven gælder både for offentlige og private virksomheder, foreninger og organisationer.

Anbefalinger til databehandleraftaler

- Forstå og implementerer kravene til en databehandleraftale
- Overhold kravene i persondataloven.

Forstå og implementer kravene til en databehandler-aftale

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

Aftalen skal indeholde:

- Hvilke specifikke databehandlinger jeres leverandør foretager.
- Hvilke typer data, der er tale om, fx CPR-nr., helbredsoplysninger mv.
- De sikkerhedsforanstaltninger, jeres virksomhed og leverandøren tager for at hindre, at oplysningerne ikke bliver lækket eller hacket.
- Hvordan I følger op på, at sikkerhedsforanstaltningerne er tilstrækkelige og bliver overholdt.
- Krav om, at leverandøren straks skal underrette jer skriftligt ved enhver afvigelse fra instrukserne i aftalen.
- Krav om, at medarbejderne hos jeres leverandør har tavshedspligt.

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

Overhold kravene i Persondataloven

Persondataloven deler personoplysninger op i tre typer, som er følsomme oplysninger, andre typer personoplysninger og almindelige personoplysninger. Se vejledning om håndtering af personoplysninger på www.sikkerhedstjekket.dk.

Hvis jeres organisation indsamler, registrerer eller videreformidler personoplysninger, betegnes jeres virksomhed som **dataansvarlig**. Det er dermed jeres ansvar at definere, hvad formålet er med at indsamle, registrere, opbevare og dele de personoplysninger, som jeres virksomhed har, samt at definere, hvilke systemer der må benyttes til behandling af personoplysningerne under jeres ansvar.

Ifølge persondataloven er det jeres virksomhed som dataansvarlig, der er ansvarlig for, at persondataloven overholdes.

Hvis I benytter en ekstern it-driftsleverandør, betegnes de som **databehandler**. Databehandleren opbevarer og behandler oplysningerne på jeres vegne. Dvs. at en databehandler skal handle efter instruks fra jeres virksomhed. Det er derfor alene jeres virksomhed, som har ansvaret for, at oplysningerne opbevares og behandles korrekt.

For at fastlægge jeres lovgivningsmæssige forpligtelser er det derfor vigtigt, at I afklarer, om I er dataansvarlige, og hvem der evt. er jeres databehandlere.

I april 2016 blev den nye databeskyttelsesforordning (General Data Protection Regulation) vedtaget, som skal være implementeret den 25. maj 2018. Forordningen stiller yderligere krav til behandling af persondata. En måde at komme godt i gang med den nye databeskyttelsesforordning på er at overholde eksisterende persondatalovgivning.

Hvis du vil vide mere

- Datatilsynets hjemmeside – hvornår er man henholdsvis dataansvarlig og databehandler?: https://www.datatilsynet.dk/erhverv/dataansvarlig-databehandler/hvornaar-er-man-henholdsvis-dataansvarlig-og-databehandler/

- Datatilsynets hjemmeside – krav om skriftlig kontrakt med databehandlere: https://www.datatilsynet.dk/erhverv/dataansvarlig-databehandler/databehandler/