RHD REVISION

TEMANUMMER FEBRUAR 2020

DIN REVISOR INFORMERER

VÆRDIFULD VIDEN OM ØKONOMI

TEMA: **IT-SIKKERHED**

Har du styr på jeres it-sikkerhed?

Mange virksomheder opbevarer følsomme data på servere, som kan hackes. Disse data kan være grundlaget for det, som giver din virksomhed konkurrencekraft og sikrer en god markedsposition. Et angreb på følsomme data kan være forretningskritisk. Derfor er it-sikkerhed efterhånden den mindst lige så vigtig en faktor som maskiner, medarbejdere og et højt serviceniveau over for kunder og samarbejdspartnere. I dette nummer af DIN REVISOR INFORMERER sætter vi fokus på it-sikkerhed.

Alt tyder på, at antallet af hackere er stigende, og at disse bliver dygtigere og snedigere. I takt med dette stiger antallet af data-indbrud, angreb og netsvindel løbende. Derfor er det yderst vigtigt, at du har styr på, hvordan din virksomhed anvender it, og hvor I skal tage jeres sikkerhedsforanstaltninger.

I dette nummer kan du blandt andet læse om forskellige former for hacker-angreb. De oftest forekommende sikkerhedsbrud sker som CEO fraud, phishing og ransomware. Ved CEO fraud sender hackeren en mail i direktørens navn til virksomhedens økonomiafdeling og beder om at få overført penge. Ved phishing forsøger de cyberkriminelle at franarre din virksomhed en række fortrolige oplysninger. Ransomware anvendes af cyberkriminelle til at inficere en brugers computer og derefter kræve en løsesum for, at virksomheden kan få adgang til sine filer.

Sikker opbevaring af følsomme data indgår som en del af GDPR-reglerne, og du skal derfor også tænke it-sikkerhed i forhold til GDPR. På side seks kan du læse om fem store faldgruber i forbindelse med GDPR-reglerne.

FIRE GODE RÅD TIL IT-SIKKERHED

"Det første, man som virksomhedsejer skal gøre, er at spørge sig selv: Hvilken slags forretning driver jeg, og hvad er det værste, som kan ske, hvis en ondsindet it-hacker ønsker at gøre skade på min virksomhed"

Troels Langkjær, it-sikkerhedsspecialist

MAN kan opstille fire generelle råd, som langt de fleste virksomheder kan have gavn af. Det første råd handler om, at man skal anvende to-trinsbeskyttelse, især når du logger ind på din mail. Råd nummer 2 handler om at opdatere sit styresystem, mens råd nummer 3 handler om at opdatere sine softwareprogrammer. Det fjerde råd er meget vigtigt og ganske banalt: Det er godt at have to backups, og det er godt at have dem liggende to forskellige steder – gerne online og offline.

LÆS SIDE 4-5

112336

CEO fraud, phishing og ransomware volder problemer

Digitaliseringen giver dig uanede nye muligheder, men trusler kan opstå, eksempelvis i form af sikkerhedsbrud. Tre af dem kan du læse om her.

De oftest forekommende sikkerhedsbrud sker som CEO fraud, phishing og ransomware. Det er angreb, som har til formål at bruge virksomhedens systemer og ansatte til økonomisk svindel. Er din virksomhed tilstrækkeligt beskyttet?

CEO fraud

CEO fraud går i sin enkelthed ud på, at en hacker franarrer din virksomhed oplysninger eller penge ved at udgive sig for at være direktøren. Det er derfor vigtigt, at din virksomhed har interne kontroller, som imødegår risikoen for CEO fraud. Interne kontroller er konkrete regler og procedurer for, hvordan pengeoverførsler håndteres, så din virksomhed undgår at blive narret af svindlerne.

Som virksomhedsejer bør du eksempelvis overveje, om din virksomhed har de rette beløbsgrænser for overførsler uden godkendelse, om de rette personer har adgang til at overføre penge, og om én medarbejder alene må overføre penge. Det er ofte en god idé at etablere godkendelse med to i forening på betalinger, eksempelvis via virksomhedens netbank. Rammes din virksomhed af CEO fraud, kan det blive dyrt. Når først din virksomhed har overført beløbet til en svindlers (ofte udenlandske) konto, overfører svindlerne beløbet videre til andre konti. Derefter vil det være så godt som umuligt at spore pengene og få dem tilbage.

Phishing

Ved phishing forsøger en cyberkriminel at franarre din virksomhed fortrolige oplysninger. Phishing foregår primært ved at sende utallige e-mails ud til intetanende personer og virksomheder. Det kan ske ved, at du eller en af dine medarbejdere modtager en mail med et link eller en vedhæftet fil, som ved et klik giver den cyberkriminelle adgang til fortrolig information eller adgang til din virksomheds it-system.

For at komme phishing-problematikken til livs kræver det, at du og dine medarbejdere har særligt fokus på jeres cybersikkerhed. Opmærksomhed om problemet og almindelig god sund fornuft er nogle af de bedste værktøjer til at øge jeres sikkerhedsniveau mod phishing.

Ransomware

Ransomware er en type af malware, som anvendes af cyberkriminelle til at inficere en brugers computer og derefter tjene penge ved at kræve en løsesum for, at brugeren kan få adgang til sine filer igen. Der kan være mange konsekvenser ved ransomware, både økonomiske og menneskelige og i værste tilfælde kan virksomhedens eksistensgrundlag helt forsvinde. Ransomware er en cybertrussel, som er stærkt stigende – nationalt og globalt. Det bedste råd mod ransomware er at have styr på backup-procedurer, så virksomhedens filer kan genskabes.

DIN REVISOR INFORMERER

UDGIVER
FSR – danske revisorer
Kronprinsessegade 8
DK-1306 København K

REDAKTION
Jan Wie,
eMBA, cand.comm. (redaktør)
Niklas Tullberg Hoff,
registreret revisor, cand.merc.aud. og partner
Kim Larsen,
statsautoriseret revisor, fagdirektør
Mads Grønnegaard,
cand. jur., skattekonsulent
Sara Sayk,
registreret revisor, cand.merc.aud. og chefkonsulent
Jan Brødsgaard,
cand.merc.aud., fagkonsulent
Robert Fosbo,
registreret revisor, cand.merc.aud.
Louise Nellemann,
statsautoriseret revisor, chefkonsulent

DESIGN OG LAYOUT
Mattias Wohlert

TRYK
Specialtrykkeriet arcorounborg

FOTO
Søren Wesseltoft

OPLAG
DIN REVISOR INFORMERER udkommer fem gange årligt i ca. 12.000 eksemplarer.

ISSN 2246-1698

Redaktionen er afsluttet den 6. januar 2020. Artiklerne i DIN REVISOR INFORMERER er formuleret i generelle vendinger og dækker ikke specifikke situationer. Informationerne bør ikke benyttes uden professionel rådgivning. Redaktionen påtager sig ikke ansvar for tab foranlediget af en gennemført handling eller undladelse af en handling på baggrund af artiklerne.

Den gode backup kan sikre virksomhedens overlevelse

Kan din virksomhed fortsætte uden kundekartotek, kontrakter og regnskabsmæssige registreringer? For langt de fleste virksomheder vil det volde store problemer, hvis sådanne vigtige data pludselig forsvinder, og det er der desværre stor risiko for.

Vigtige data kan gå tabt, når en harddisk crasher, eller når en medarbejder utilsigtet kommer til at slette vigtige filer. I dag er der også stor risiko for ondartede cyberangreb, hvor eksempelvis malware ødelægger virksomhedens data, og hvor ransomware låser virksomhedens computere og først åbner igen, når virksomheden har betalt løsepenge.

Backup er ikke bare backup

Hvis virksomheden har en ordentlig backup, kan vigtige data genskabes, så virksomheden hurtigere og nemmere kommer op at køre normalt igen. Uden en ordentlig backup sidder du med en reel risiko for, at din virksomhed ikke overlever.

BACKUP

En digital kopi af virksomhedens vigtigste data, eksempelvis kundekartotek, kontrakter og økonomiske data. En backup kan eksempelvis lagres på en ekstern fysisk harddisk eller i clouden.

Nogle enkle gode råd:

- **OVERVEJ VIRKSOMHEDENS** konkrete behov for backup og søg råd og vejledning, hvis der ikke er tilstrækkelige it-kompetencer i virksomheden.
- **AUTOMATISK BACKUP** er ofte en fordel. Når det først er sat op, sker den løbende backup automatisk uden menneskelig indgriben. Så bliver det gjort, uanset om du har travlt med alt muligt andet. Så kan du fokusere på din virksomhed, dine kunder og andre forhold, der skaber værdi.
- **VIRKSOMHEDENS BACKUP** skal isoleres fra virksomhedens øvrige it-systemer. Dermed undgår virksomhedens backup at blive inficeret af malware eller ransomware, hvis it-systemet rammes af cyberangreb.
- **DET ER** ofte en fordel at have flere kopier af backup på forskellige medier, eksempelvis en ekstern harddisk eller i clouden. Opbevar den ene backup et sikkert sted uden for virksomheden, så denne backup er beskyttet, hvis din virksomhed rammes af tyveri, oversvømmelse, brand eller andre katastrofer.
- **TEST PERIODISK** at din backup virker, som den skal. Testen skal sikre, at backupen indeholder alle tiltænkte data, og at din virksomhed faktisk er i stand til at gendanne data og systemer, hvis ulykken rammer.

TEGN EN CYBERFORSIKRING INDEN DU HAR BRUG FOR DEN

DIN virksomhed er et oplagt mål for cyberangreb uanset størrelse, så længe du bruger internettet. Overvej, om du skal tegne en cyberforsikring på linje med, at du også har eksempelvis en ansvarsforsikring. Inden du tegner en cyberforsikring, skal du være ekstra opmærksom på de forpligtelser, du har, hvis du oplever et cyberangreb, og hvad begrænsningerne er for dækningen.

Kortlæg din virksomheds it-sårbarhed

Hvad angår IT-sikkerhed, vil enhver virksomhed være forskellig. Derfor er det vigtigt at tage udgangspunkt i netop de it-forhold, som karakteriserer din virksomhed. Som det første skal du stille spørgsmålet: Hvad er det værste, der kan ske, hvis min virksomhed bliver offer for et it-angreb?

Undersøgelser viser, at stadig flere danske virksomheder udsættes for cyberkriminalitet, og cybersikkerheden er ofte lav i små og mellemstore virksomheder. DIN REVISOR INFORMERER har derfor sat cybersikkerhedsekspert Troels Langkjær i stævne for at få gode råd til, hvordan små og mellemstore virksomheder bør forholde sig til truslen fra hackere.

"Det første, man som virksomhedsejer skal gøre, er at spørge sig selv: Hvad er det værste, der kan ske, hvis en hacker ønsker at gøre skade på min virksomhed", lyder den indledende replik fra Troels Langkjær, som er uddannet datalog og i en årrække har arbejdet med it-sikkerhed i NNIT, Mærsk, forsvaret og som iværksætter og rådgiver. Han fortsætter:

"Det indebærer at gøre sig selv klart, hvor og hvordan ens vigtigste forretningsgange er digitaliserede"

Virksomhedens anvendelse af it

Troels Langkjær påpeger, at nogle virksomheder har digitaliseret centrale dele af produktionen, hvilket betyder, at fokus på sikkerheden i netop de elementer skal tages i særskilt betragtning. Andre virksomheder bruger eksempelvis deres hjemmeside til hovedparten af ordrebestillinger, og i de tilfælde skal man naturligvis bygge it-forsvaret op omkring hjemmesiden. Der vil derfor være forskel på, hvad en tømrermester, en lokal biograf og en produktionsvirksomhed skal være opmærksomme på.

Fire gode råd til den it-ansvarlige

Når det er sagt, kan man stadig opstille generelle råd, som langt de fleste virksomheder kan have gavn af. Troels Langkjær henviser til den australske regering, som har sat sig for at være førende inden for at offentliggøre konkrete råd og vejledninger, og med mange års erfaringer bag

STIGNING I ANTALLET AF SIKKERHEDSHÆNDELSER

Den globale konsulent- og revisorvirksomhed pwc har gennemført en undersøgelse, hvor 325 danske virksomhedsledere, it-chefer og specialister har svaret på, hvilke it-mæssige udfordringer de stod overfor i 2019. 51 procent angiver, at de har været udsat for en eller flere sikkerhedshændelser inden for det seneste regnskabsår. Sammenlignet med 2018 er der tale om en stigning på syv procentpoints. 76 procent svarer, at ledelsen i nogen eller i høj grad har fokus på balancen mellem cybertrusler og investeringer i cybersikkerhed.

Derudover mener 50 procent, at GDPR har været en byrde for forretningen. Undersøgelsen viser desuden, at større virksomheder har et gennemsnitligt cybersikkerhedsbudget på cirka 19 millioner kroner årligt, mens de mindre virksomheders tilsvarende budget er på 700.000 kroner. 33 procent i de mindre virksomheder svarer, at de har været udsat for mindst en sikkerhedshændelse inden for det seneste regnskabsår, mens 29 procent angiver, at de har oplevet en eller flere sikkerhedshændelser, der var målrettet deres virksomhed.

Kilde: *pwc: Cybercrime Survey 2019*

sig peger på fire tiltag til alle, der ønsker at styrke forsvaret mod cyberkriminalitet.

"Råd nummer 1 handler om, at du skal anvende to-trinsbeskyttelse, især når du logger ind på din mail, eksempelvis Outlook eller Gmail. Det kan være via en sms eller en app, hvor du får en engangskode, som du skal bruge sammen med dit password for at logge ind. Et eksempel på to-trins beskyttelse er NemID, hvor du skal bruge kodeord og nøglekort. Et andet eksempel er et internetkøb, hvor du skal taste dankortoplysninger efterfulgt af en talkode, som du har modtaget via SMS. De cyberkriminelle går ofte efter at hacke mail-konti, så det er vigtigt at være ekstra påpasselig her", forklarer Troels Langkjær og fortsætter:

"Råd nummer 2 handler om at opdatere sit styresystem, mens råd nummer 3 handler om at opdatere sine softwareprogrammer."

Råd nummer 4 er yderst velkendt, men ikke desto mindre værd at gentage igen og igen. Det drejer sig om at tage backup.

"Det fjerde råd er også afgørende vigtigt og ganske banalt, men djævlen kan dog stadig ligge i detaljen. Det er godt at have to back ups, og det er godt at have det liggende to forskellige steder. Det må meget gerne være sådan, at den ene backup er online og den anden er offline, eksempelvis på en harddisk, som ikke er tilsluttet et netværk."

Afslutningsvis henviser Troels Langkjær til, at Erhvervsstyrelsen sammen med Digitaliseringsstyrelsen har samlet god, brugbar viden om digital sikkerhed, som du kan finde på hjemmesiden www.sikkerdigital.dk, hvor du kan se en række cases fra danske virksomheder, som har været ramt af hackerangreb. Hjemmesiden skal ses som en guide til danske virksomheder, som ønsker en it-sikkerhedsmæssig oprustning.

IT-SIKKERHEDSTJEKLISTE

DET australske it-sikkerhedscenter Australian Cyber Security Centre (ACSC) har opstillet fire gode råd og udfærdiget en tjekliste, som du kan bruge i bestræbelserne på at komme hackere til livs. De fire råd relaterer sig til teknologi og software, hvilket betyder, at det typisk er din virksomheds it-ansvarlige eller eksterne it-leverandører, som kan hjælpe med anbefalingerne.

- Brug to-trinsbeskyttelse
- Sæt dine systemer op, så du automatisk og ofte opdaterer dine softwareprogrammer
- Sæt dine systemer op, så du automatisk og ofte opdaterer dit styresystem
- Lav daglig backup af dine data

DERUDOVER opstiller ACSC yderligere fire gode råd, som relaterer sig til din virksomheds procedurer.

- Vær opmærksom på, hvordan administrationsrettigheder er tildelt i organisationen, og begræns den enkelte medarbejders rettigheder til det nødvendige.
- Anvend stærke brugernavne og passwords. Disse skal være komplekse, lange, unikke og lette at huske. Brug dem sammen med to-trinsbeskyttelse.
- Gør medarbejdere opmærksomme på vigtigheden af cybersikkerhed og giv anvisninger til, hvordan de kan være med til at dæmme op for eventuelle hackerangreb.
- Hav en plan klar, hvis uheldet skulle være ude.

Kilde: Australian Cyber Security Centre: Small business Cyber Security Guide, oktober 2019.

Guiden kan downloades på www.cyber.gov.eu, hvor du også kan læse meget mere om cybersikkerhed.

GDPR:
Fem faldgruber

Når du arbejder med at sikre, at din virksomhed lever op til GDPR-lovgivningen, kan det være svært at finde hoved og hale i de mange paragraffer. Læs her om fem faldgruber, som du kan risikere at falde i, når du arbejder med at gøre din virksomhed GDPR-klar.

"Jeg har ingen personfølsomme oplysninger". Dette udsagn hører man ofte fra virksomhedsejere, der bliver spurgt, om der er styr på GDPR. Du og din virksomhed er omfattet af GDPR, hvis I har en ansat, en kunde eller en leverandør. GDPR omhandler personhenførbare oplysninger og kan deles op i almindelige oplysninger og personfølsomme oplysninger.

Du må gerne have persondata i din virksomhed
Vi ønsker som individer ikke, at vores data kan tilgå uvedkommende. Som virksomhedsejer må du således påtage dig ansvaret og behandle og opbevare personoplysninger med ansvar og respekt. Du må gerne have personoplysninger, når blot du har et formål med at opbevare dem samt en hjemmel og ved, hvornår du skal slette oplysningerne. Det er måden, du håndterer data, hvad du bruger dem til, og hvordan du dokumenterer behandlingen af oplysningerne, der er blevet skærpet.

FEM FALDGRUBER

Ligesom kokken skal tjekke temperaturen i køleskabet, skal du også sikre, at din virksomhed lever op til lovgivningen. De typiske faldgruber er:

- **Den lovpligtige interne fortegnelse**
  GDPR kræver, at I har en intern fortegnelse over alle personoplysninger, som I opbevarer og behandler. Du skal løbende opdatere denne og videregive den til Datatilsynet på forlangende.
- **Nedprioritering af GDPR-opgaven**
  Nogle virksomheder har svært ved at forholde sig til GDPR og skubber derfor opgaven foran sig. Hvis du ikke tager GDPR alvorligt, kan din virksomhed få en bøde af en betydelig størrelse. Bøden er en ting i sig selv, mens et dårligt ry og omdømme for din virksomhed kan have fatale konsekvenser.
- **Misforståelser eller mangel på viden**
  De færreste virksomheder har haft tid til at sætte sig ind i, hvad der kræves for at leve op til lovgivningen.
- **Dine medarbejdere er ikke klædt ordentlig på**
  Du har pligt til at dokumentere, at dine medarbejdere har fået ordentlig instruktion i, hvordan personoplysninger skal behandles. Hovedparten af de 3.500 anmeldelser til Datatilsynet, der omhandler sikkerhedsbrud, er sket på grund af menneskelige fejl.
- **Sletning er ikke sat i system**
  Du må gerne opbevare persondata, så længe der er et formål, og du har en hjemmel, der understøtter formålet. Når formålet med at opbevare persondata ophører, skal I slette personoplysningerne. Det er vigtigt, at I laver en slettepolitik og følger denne. I de kendte sager i Danmark er det netop slettepolitikken eller manglen på samme, der har udmøntet sig i bøder.

De første politianmeldelser har set dagens lys

ID Design og Taxa 4x35 er af datatilsynet blevet anklaget for ikke at overholde GDPR-reglerne. Læs her om anklagens indhold.

HVIS du ikke rettidigt sletter personoplysninger og ikke fastsætter passende slettefrister for de personoplysninger, som din virksomhed behandler, kan dette få både økonomiske konsekvenser og skade virksomhedens omdømme. Dette har både ID Design og Taxa 4x35 erfaret, da Datatilsynet kom på besøg.

ID Design havde ikke forholdt sig til sletning af deres kundeoplysninger

ID Design havde ikke overholdt GDPR-reglerne om sletning af personoplysninger i tre gamle økonomisystemer, hvor de havde behandlet op imod 385.000 kundeoplysninger. Virksomheden havde ikke taget stilling til, hvornår personoplysningerne i det gamle system ikke længere var nødvendige til det formål, hvortil de blev behandlet. Der var tale om kundens navn, adresse, telefonnummer, e-mail og købshistorik. Datatilsynet indgav derfor en politianmeldelse til Østjyllands politi og indstillede ID Design til en bøde på 1,5 millioner kroner. Herudover udtalte Datatilsynet en alvorlig kritik i forhold til virksomhedens manglende slettefrister og manglende procedurer for sletning af personoplysninger.

Taxa 4x35's manglende slettefrister

Datatilsynet har ligeledes undersøgt, om Taxa 4x35 havde fastsat frister for sletning af kundernes oplysninger, og om disse frister blev efterlevet. Her var problemet, at selskabet ikke rettidigt havde slettet kundens telefonnummer efter to år, som de ellers havde gjort det med kundens navn. Telefonnummeret blev først slettet efter fem år, da man brugte dette til at få oplysninger om kundens taxature. Datatilsynet fandt, at opbevaringen af telefonnumrene ikke var nødvendig, og derfor udtalte de alvorlig kritik af selskabets håndtering af persondata og anmeldte virksomheden til politiet.

Vær opmærksom på rettidig sletning

Personoplysninger skal slettes,

- når det ikke længere er nødvendigt at have oplysningerne
- når den registrerede trækker sit samtykke, eller samtykket forældes
- når din virksomhed behandler oplysningerne ulovligt
- når lovgivning forpligter din virksomhed til at slette oplysningerne. Eksempelvis hvidvasklovens krav om sletning efter fem år og krav om sletning af samtykke efter to år, medmindre samtykket fornys
- når den registrerede beder om det.

BEGREBER

DATAANSVARLIG

En dataansvarlig er den, der bestemmer med hvilke formål personoplysningerne må behandles (formålet), og hvordan personoplysningerne må behandles (hjælpemidlerne), herunder af hvem personoplysningerne må behandles.

ALMINDELIGE PERSONOPLYSNINGER

Almindelige personoplysninger omfatter alle oplysninger, der ikke er klassificeret som særlige kategorier af oplysninger (personfølsomme oplysninger). Det kan for eksempel være identifikationsoplysninger som navn og adresse eller oplysninger om økonomi, skat, gæld, væsentlige sociale problemer, andre rent private forhold, sygedage, tjenstlige forhold, familieforhold, bolig, bil, eksamen, ansøgning, CV, ansættelsesdato og -stilling, arbejdsområde og arbejdstelefon.

PERSONFØLSOMME OPLYSNINGER

Følsomme oplysninger er oplysninger om race og etnisk oprindelse, politisk overbevisning, religiøs eller filosofisk overbevisning, fagforeningsmæssige tilhørsforhold, genetiske data, biometriske data med henblik på entydig identifikation, helbredsoplysninger og seksuelle forhold eller seksuel orientering.

Kilde: Datatilsynet

R+D REVISION
Registreret Revisionsaktieselskab
Erhvervsvej 2 • 8721 Daugård • Tlf. 75 89 60 66 • info@r-i-d.dk • www.r-i-d.dk

VIGTIGE DATOER

JANUAR 2020

15. Lønsumsafgift (kvartal + måned)
17. A-skat + AM-bidrag lønmodtagere (små+mellem), indberetning af e-Indkomst (små+mellem)
20. B-skat + AM-bidrag selvstændige
27. Månedsmoms (store), EU-salg uden moms (små+mellem+store) (kvartal + måned)
31. A-skat + AM-bidrag lønmodtagere (store), indberetning af e-Indkomst (store)

FEBRUAR 2020

1. Acontoskat (selskaber)
7. ATP, Feriekonto (timelønnede)
10. A-skat + AM-bidrag lønmodtagere (små+mellem), indberetning af e-Indkomst (små+mellem)
17. Lønsumsafgift (måned)
20. B-skat + AM-bidrag selvstændige
25. Månedsmoms (store), EU-salg uden moms (store)
28. A-skat + AM-bidrag lønmodtagere (store), indberetning af e-Indkomst (store)

MARTS 2020

2. Halvårsmoms (små), kvartalsmoms (mellem)
10. A-skat + AM-bidrag lønmodtagere (små+mellem), indberetning af e-Indkomst (små+mellem)
16. Lønsumsafgift (måned)
20. B-skat + AM-bidrag selvstændige, acontoskat (selskaber)
25. Månedsmoms (store), EU-salg uden moms (store)
31. A-skat + AM-bidrag lønmodtagere (store), indberetning af e-Indkomst (store)

APRIL 2020

14. A-skat + AM-bidrag lønmodtagere (små+mellem), indberetning af e-Indkomst (små+mellem)
15. Lønsumsafgift (kvartal+måned)
20. B-skat + AM-bidrag selvstændige
27. Månedsmoms (store), EU-salg uden moms (små+mellem+store) (kvartal+måned)
30. A-skat + AM-bidrag lønmodtagere (store), indberetning af e-Indkomst (store)

GODT AT VIDE

STRAKSAFSKRIVNING 2020

Maksimumgrænse for straksafskrivning af småaktiver . . . . . 14.100 kr.

BEFORDRINGSFRADRAG 2020

0-24 km: . . . . . 0 kr.
24-120 km: . . . . . 1,96 kr.
Over 120 km: . . . . . 0,98 kr.

KØRSELSGODTGØRELSE 2020

Egen bil eller motorcykel pr. km
Indtil 20.000 km . . . . . 3,52 kr.
Over 20.000 km . . . . . 1,96 kr.
Egen cykel eller knallert pr. km . . . . . 0,54 kr.

ARBEJDSGIVERNES DAGPENGEGODTGØRELSE, 2020

Pr. dag: . . . . . 881 kr.

SYGEDAGPENGE 2020

Max. pr. uge: . . . . . 4.405 kr.

Yderligere oplysninger: www.bm.dk

REJSEGODTGØRELSE 2020

Logi – efter regning eller pr. døgn . . . . . 223 kr.
Fortæring pr. døgn . . . . . 521 kr.
Tilsluttende døgn pr. time . . . . . 21,71 kr.
Fri morgenmad . . . . . 78,15 kr.
Fri frokost . . . . . 156,30 kr.
Fri middag . . . . . 156,30 kr.
25 pct. godtgørelse . . . . . 130,25 kr.

NETTOPRISINDEKS 2019

December 2019 103,4
November 2019 103,6
Oktober 2019 103,8
September 2019 103,4
August 2019 103,7
Juli 2019 104,1
Juni 2019 103,4
Maj 2019 103,6
April 2019 103,7
Marts 2019 103,4
Februar 2019 103,3
Januar 2019 102,6

Bemærk: Fra og med januar 2016 er referenceperioden (basisåret) 2015. Dermed er 2015 = 100.

Yderligere oplysninger: www.dst.dk/priser

Riv ud og gem