et trygt samfund med it og data

Revisorerklæring

C-SOLUTION ApS

ISAE 3402 type 1 erklæring om generelle it-kontroller
pr. 27. januar 2022 relateret til drift af hostingplatform

REVI-IT A/S | www.revi-it.dk
Højbro Plads 10, 1200 København K
CVR: 30 98 85 31 | Tlf. 33 11 81 00 | info@revi-it.dk
www.dpo-danmark.dk | www.revi-cert.dk

Februar 2022

Indholdsfortegnelse

Afsnit 1: Beskrivelse af C-SOLUTION ApS' ydelser i forbindelse med drift af hosting-platform samt generelle it-kontroller relateret hertil

Beskrivelse af C-SOLUTION ApS' ydelser i forbindelse med drift af hostingplatform

I det følgende beskrives C-SOLUTION ApS' ydelser til kunder, som er omfattet af de generelle it-kontroller, som erklæringen omhandler. Erklæringen omfatter generelle processer og systemopsætninger m.v. hos C-SOLUTION ApS. Processer og systemopsætninger m.v., der er individuelt aftalt med C-SOLUTION ApS' kunder er ikke omfattet af erklæringen. Vurdering af eventuelle kundespecifikke processer og systemopsætninger m.v. vil fremgå af specifikke erklæringer til kunder, der har bestilt sådanne.

Kontroller i applikationssystemer er ikke omfattet af denne erklæring.

Generelle it-kontroller hos C-SOLUTION ApS

Indledning

C-SOLUTION ApS beskæftiger 17 medarbejdere og er inddelt i afdelingerne salg, support, IT-Drift, marketing og ledelse. Support modtager størstedelen af de indkommende forespørgsler fra kunderne og løser kundernes problemer eller videreformidler problemet til IT-Drift, hvis problemet relaterer sig til hertil. Den ansvarlige for supportafdelingen er Jonas Bach. IT-Drift modtager også forespørgsler fra kunderne, men disse relaterer sig udelukkende til IT-Drifts ansvarsområde. IT-Drift håndterer herudover den praktiske implementering af nye kunder, IT-sikkerheden i C-SOLUTION ApS, overvåger bestående driftsløsninger og andre opgaver, der relaterer sig til den daglige drift af C-SOLUTION ApS' IT-løsninger. Brian Pedersen er ansvarlig for IT-Drift. Der eksisterer et tæt sammenspil mellem support-afdelingen og IT-Drift afdelingen omkring løsning af kundens problemer.

Salgsafdelingen står for alle aktiviteter, der knytter sig til salg til nye kunder eller mersalg til eksisterende kunder samt vedligeholdelse af kunderelationer og opsætning af kundeløsninger. Salgsafdelingen består derfor også af montører, der har ansvar for alle opgaver, der relaterer sig til opsætning af løsninger ude hos kunden. Montørerne arbejder sammen med IT-Drift og support om at drifte de fysiske løsninger, som C-solution sælger og opsætter. Den ansvarlige for salgsafdelingen er Brian Pedersen.

Marketing arbejder med bl.a. C-SOLUTION ApS' SoMe, SEO, hjemmeside, branding og kunderelationer. Marketing arbejder derfor ofte sammen med salgsafdelingen og ledelsen i udformningen af salgs- og brandingmateriale. Den ansvarlige for marketingsafdelingen er Henrik Kristjansen.

Ledelsen har bl.a. ansvaret for strategi, koordinering på kryds af afdelingerne, den fysiske sikkerhed, kapacitetsstyring og økonomi. Ledelsen arbejder således tæt sammen med alle afdelingerne i C-solution omkring interne såvel som kundevendte opgaver. Ledelsen består af CEO; Brian Pedersen og CFO; Henrik Kristjansen.

Anvendelse af underleverandører

C-SOLUTION ApS anvender underleverandørerne Teamblue A/S samt Cloud.factory A/S i forbindelse med leverancen af hostingplatform til kunder.

Generelt om vores kontrolmål og implementerede kontroller
Vi har defineret vores kvalitetsstyringssystem ud fra vores overordnede målsætning om at levere stabil og sikker IT-drift til vores kunder. For at kunne gøre det, er det nødvendigt, at vi har indført politikker og procedurer, der sikrer, at vores leverancer er ensartede og gennemsigtige.

Vores it-sikkerhedspolitik er udarbejdet med reference til ovenstående og er gældende for alle medarbejdere og for alle leverancer.

Vores metodik for implementering af kontroller er defineret med reference til ISO 27002 (Regelsæt for styring af informationssikkerhed), og er dermed helt overordnet inddelt i følgende kontrolområder:

5. Informationssikkerhedspolitik
6. Organisering af informationssikkerhed
7. Sikkerhed i forhold til HR
8. Styring af aktiver
9. Adgangskontrol
10. Kryptografi
11. Fysisk og miljømæssig sikring
12. Sikkerhed i forbindelse med drift
13. Kommunikationssikkerhed
15. Leverandørforhold
16. Styring af sikkerhedshændelser
17. Informationssikkerhedsaspekter ved beredskabsstyring
18. Overensstemmelse

Vi foretager løbende forbedringer af både politikker, procedurer og den operationelle drift.

Risikovurdering og -håndtering

IT-risikoanalyse
Det sikkerhedsniveau, denne politik repræsenterer, er fastsat på baggrund af C-SOLUTION ApS' vurdering af de forretningsmæssige IT-risici, som vi ønsker at imødegå. IT-risikovurderingen opdateres årligt og ved eventuelle større ændringer i IT-systemerne, ændringer i anvendelse af systemerne eller ved større organisatoriske ændringer med efterfølgende tilretning af informationssikkerhedspolitikken, retningslinjer mm. Ansvarlige for området CFO: Henrik Kristjansen og CEO: Brian Pedersen

Procedure for risikohåndtering
Vi har processer på plads, der dækker opdagelse, klassificering, håndtering og opfølgning af sikkerhedshændelser. Processerne overvåges af vores driftschef, der sikrer, at sikkerhedshændelserne behandles rettidigt ud fra den vurderede impact og urgency. Til hvert klassificeringsniveau er der fastlagt en procedure for håndtering af sikkerhedshændelsen, der sikrer, at vi følger best practice. Efter håndtering af sikkerhedshændelsen har vi klare retningslinjer for opfølgningen, der sikrer, at vi får evalueret om sikkerhedshændelsen blev håndteret hensigtsmæssigt, og om sikkerheden er genoprettet.

IT-sikkerhedspolitik
Vi har i C-SOLUTION ApS defineret præcise retningslinjer for levering af vores ydelser, i vores IT-sikkerheds-politik og tilhørende strategiske og taktiske dokumenter. Ligeledes er der fastlagt kontroller for at sikre, at der nedsættes rettidige sanktioner i tilfælde af overtrædelser, og at IT-sikkerhedspolitikken holdes ajour i takt med, at vi udvikler os, hvilket er sikret i vores IT-sikkerhedsgruppe. Formålet er at sikre, at vi følger IT-drift- og ledelsesgodkendte retningslinjer for informationssikkerhed i forhold til vores strategier, forret-ningsmål og relevant lovgivning.

Evaluering af IT-sikkerhedspolitikken
Vi opdaterer løbende IT-sikkerhedspolitikken, og hver år i december afholdes internt møde for gennemgang og revidering af politikken. Til dette møde deltager CEO samt IT -sikkerhedsgruppen.

6. Organisering af informationssikkerhed

Intern organisering

Delegering af ansvar for informationssikkerhed
Vi har en klar opdelt organisation, hvad angår ansvar, og har ansvars- og rollebeskrivelser på alle niveauer lige fra ledelsesniveau til de enkelte driftsmedarbejdere.

Funktionsadskillelse
I C-SOLUTION ApS er vi opmærksomme på at minimere afhængigheden af nøglepersoner. Dette betyder konkret, at der sikres mod individuelt ejerskab af de anvendte systemer, og gennemsigtighed når der fore-tages ændringer. Funktionsadskillelse er en vigtig del af at minimere denne afhængighed, hvorfor vi i C-SO-LUTION ApS har nedsat adgangskontroller og rettighedsstyring, der sikrer, at medarbejderne kun kan ud-føre handlinger i vores systemer, der knytter sig til deres funktion. Hertil er der registrerede administratorer for hvert system, der øger gennemsigtigheden af, hvem der foretager ændringer.

Informationssikkerhed som en del af projektstyring
I de projekter som vi udfører for vores kunder, er IT-sikkerhed altid en faktor, der bliver taget stilling til, uanset projektets størrelse eller type.

Mobilt udstyr og fjernarbejdspladser

Politik for mobile enheder
C-SOLUTION ApS har en fast politik, der tager udgangspunkt i CIS20 og som danner rammerne for medar-bejdernes anvendelse af laptops uden for virksomheden. IT hører under den overordnede IT-sikkerhedspoli-tik. Dette sikrer bl.a., at vores laptops er beskyttet af logon og virusbeskyttelse.

Vi har faste kontroller, der sikrer, at anvendelsespolitikken holdes opdateret i forhold til vores udvikling.

Fjernarbejdspladser
Gennem vores medarbejderhåndbog er medarbejderne i C-SOLUTION ApS informeret om retningslinjerne for fjernarbejde, og der er fastlagte rammer for hvilke enheder, der må tilgå C-SOLUTION ApS' interne net-værk.

Medarbejdere, der arbejder hjemme, er sikret via VPN.

7. Sikkerhed i forhold til HR

Inden ansættelse

Screening
Nye medarbejdere i C-SOLUTION ApS screenes før ansættelse gennem tjek af deres straffeattest efter en fast procedure, suppleret af referencer, hvor det er relevant og muligt. Nye medarbejdere gøres fra start bevidst om deres ansvarsområde i C-SOLUTION ApS og virksomhedens værdier. Samarbejde med konsulenter og freelancere sker gennem klare retningslinjer for ansvar og sikkerhed samt krav til kvaliteten af samarbejdet.

Ansættelsesforhold
Vi sikrer, at alle intellektuelle rettigheder tilhører virksomheden eller dens kunder. Ligeledes er vores medarbejdere underlagt regler om fortrolighed angående data fra virksomheden og virksomhedens kunder.

Under ansættelse

Ledelsens ansvar
Ansættelse af medarbejdere følger en fast proces i forhold til ansættelsesvilkår. Hertil har vi klare rammer for overtrædelse af informationssikkerhedspolitikken og den efterfølgende håndtering. Ligeledes er det CEO og CFO, der har ansvaret for at informere medarbejderen i tilfælde af overtrædelser af den gældende kontrakt, der derfor bryder virksomhedens politikker og procedurer og eventuelle konsekvenser, der måtte følge af disse overtrædelser. Udvidelse af en medarbejders ansvarsområde eller rolle sker ved medarbejderens accept af en forespørgsel fra CEO eller CFO. Vi sørger for, at vores medarbejdere løbende udvikles i forhold til best practice inden for deres ansvarsområde og informationssikkerhedspolitik.

Bevidsthed om, uddannelse og træning i informationssikkerhed
I C-SOLUTION ApS er det afdelingen, der arbejder med IT-Drift, der står for at uddanne resten af virksomheden i informationssikkerhed. Der er hertil kontroller på plads, der sikrer, at medarbejderne informeres om informationssikkerhed.

Medarbejderne holdes således ajour med sikkerhed og bevidste om potentielle trusler rettidigt. Hertil er det CEO og CFO, der sørger for, at IT-Drift har de rigtige kvalifikationer til at bære dette ansvar gennem certificeringer og kurser. Derudover sørger CEO og CFO for, at medarbejderne har de rigtige certificeringer og kurser inden for deres givne ansvarsområde. Eksterne parter, som C-SOLUTION ApS samarbejder med, inden for IT-Drift inkluderer vi ligeledes i disse sikkerhedsretningslinjer og orienterer dem, så snart der sker ændringer.

Sanktioner
I C-SOLUTION ApS er der processer på plads, der sikrer, at sanktioner udføres effektivt og rettidigt. CEO & CFO er øverste myndighed i forhold til sanktioner og er således de eneste, der kan sanktionere.

Ophør og ændring i ansættelse
Der er en fast proces til at sikre, at medarbejdere tilbageleverer alle data og informationsaktiver, som medarbejderen har fået udleveret under ansættelse i C-Solution. CFO har ansvaret for de overordnede kontroller. Ved ændring i ansættelse har medarbejderen krav på at indlevere de aktiver og brugeroplysninger til systemer, der ikke knytter sig til medarbejderens nye ansættelsesvilkår og rolle. Hertil lukkes medarbejderens tidligere rolle, før nye beføjelser gives.

8. Styring af aktiver

Fortegnelse over aktiver
Vi har fastlagte procedurer for registrering og udlevering af informationsaktiver til internt brug, der sikrer, at vores informationsaktiver har et tilknyttet ejerskab i form af en medarbejder, der har ansvaret for det pågældende informationsaktiv. Hertil har vi et etableret system til fortegnelse over aktiver, så det er synligt hvilke aktiver, der er på lageret og hvilke aktiver, der kan findes hos den enkelte medarbejder.

Ejerskab af aktiver
C-SOLUTION ApS bruger sikkerhedsgodkendte underleverandører til hosting af servere. Der tjekkes årligt op på, at vores underleverandører lever op til C-SOLUTION ApS' sikkerhedskrav.

Acceptabel brug af aktiver
Vi har i C-SOLUTION ApS en IT-politik på plads, der sikrer, at vores medarbejdere er informeret om, og har accepteret konkrete vilkår for acceptabelt brug af de aktiver, som de får udleveret. Vores IT sikkerheds-gruppe holder IT-politikken ajour med udviklingen af de aktiver, som C-SOLUTION ApS tilbyder medarbejde-ren.

Tilbagelevering af aktiver
Fratræder en af vores medarbejdere har vi en udførlig procedure, der sikrer, at medarbejderen indleverer alle relevante aktiver, som medarbejderen har fået udstedt i løbet af sin ansættelse. Proceduren sikrer også, at medarbejderens adgangsrettigheder fjernes rettidigt.

Dataklassifikation

Klassifikation af data
De data, som ligger på vores og vores kunders servere, bliver klassificeret således, at dataenes fortrolighed tages i betragtning. Dette afspejler sig i de backups, vi foretager, som følger en fastlagt procedure, der også bestemmer hyppigheden af backups og tilgængeligheden af førnævnte data.

Mærkning af data
Klassificeringen er dokumenteret og opdateres rettidigt dog minimum årligt. Vores kunders data er klassifi-ceret sammen på et niveau, der matcher vores klassifikation af egne data, mens systemdata for netværk dokumentation er prioriteret højest herunder sikret betryggende vis.

Håndtering af aktiver
Beskyttelse af vores kunders data og deres systemer samt vores egne data og systemer har højeste priori-tet. Vi håndterer derfor ikke kunders data på håndbårne medier (USB-nøgler, CD/DVD) uden forudgående aftale med kunden og passende fysisk beskyttelse mod miljø, hærværk og tyveri.

Mediehåndtering

Styring af bærbare medier
Gennem vores IT-anvendelsespolitik sikrer vi, at alle medarbejdere er indforstået med, hvordan de håndte-rer og anvender bærbare medier samt er informeret om den sikkerhedsmæssige konfiguration og regler for opdatering med henblik på nye sikkerhedstiltag. Politikken revideres årligt af IT-sikkerhedsgruppen for at holde den opdateret i forhold til virksomhedens udvikling.

Bortskaffelse af medier
Vi har et etableret samarbejde med en tredjepartsvirksomhed, som er ansvarlig for destruktion og bortskaffelse af medier og tilhørende data, hvorefter der sendes en bekræftelse fra virksomheden på, at destruktionen og bortskaffelsen er udført.

9. Adgangskontrol

Politikker for adgangsstyring
Vi har i C-SOLUTION ApS en fastlagt politik omkring adgangsstyring ved- og under ansættelse samt ved fratrædelse. Dette mindsker sandsynligheden for misbrug af vores kunders data samt øger sporbarheden og gennemsigtigheden.

Adgang til netværk og netværksservices
I C-SOLUTION ApS inddeles medarbejdere i sikkerhedsgrupper, der har forskellige adgangsniveauer I forhold til netværksservices. Tildelingen af adgang sker med udgangspunkt i sikkerhedsgrupperne, hvorigennem medarbejderne udelukkende får adgang til de netværksservices, der er passende for deres ansvarsområde.

Administration af brugeradgange

Brugeroprettelses- og nedlæggelsesprocedure
I C-SOLUTION ApS oprettes interne brugere på baggrund af medarbejdernes behov, der knytter sig til deres ansvarsområde.

I de løsninger som vi leverer, oprettes brugere på baggrund af kundens ønske med mulighed for at konsultere C-SOLUTION ApS.

Ved fratrædelse har vi procedurer, der sikrer, at medarbejderen fratages sine rettigheder til kunde og persondata. Ligeledes tilbageleveres alt udstyr, der er blevet udleveret til medarbejderen, og delte passwords ændres.

Rettighedstildeling
Tildeling af yderligere rettigheder er kontrolleret af C-SOLUTION ApS' systemejer med godkendelse fra CFO.

Kontrol med privilegerede adgangsrettigheder
Anvendelse af passwords følger en fastlagt procedure og faste retningslinjer omkring længde, kompleksitet og fornyelse.

Håndtering af fortrolige logon informationer
Vi informerer vores medarbejdere i håndtering af fortrolige informationer herunder logon information mv.

Evaluering af brugeradgangsrettigheder
Det tjekkes halvårligt, at ingen fratrådte medarbejdere har rettigheder eller adgang til virksomhedens data.

Nedlæggelse eller tilpasning af adgangsrettigheder
Nedlæggelse og tilpasning af rettigheder følger faste procedurer.

Brugeransvar
Vores IT-sikkerhedspolitik foreskriver, at vores medarbejderes kodeord er personlige, og det er alene brugeren selv, der må kende kodeordet. Ligeledes ibrugtages to-faktor godkendelse til logon. Medarbejderne skriver årligt under på, at de har læst og forstået seneste version af vores IT-sikkerhedspolitik.

Vi bruger et system til opbevaring af delte og personlige passwords, der beskytter den enkelte medarbejders passwords fra andre i virksomheden, men samtidig giver adgang til de delte passwords, som medarbejderne har autoritet til. Kun autoriseret personale har administratoradgang til password opbevaringssystemet. Der stilles højere krav for medarbejderens password til dette system end for den almindelige password politik.

Kontrol af adgang til systemer og data

Begrænset adgang til data
Vores medarbejdere har udelukkende adgang til de data og systemer, der knytter sig til deres ansvarsområde og daglige arbejde, hvorfor medarbejderens adgang til andre systemer og data er begrænset. Kundernes brugeradgang til kundens systemer og data fastlægges ud fra kunden.

Procedurer for sikkert log-on
Vores medarbejdere bruger passwords og to-faktor godkendelse til at logge på vores systemer.

System for administration af adgangskoder
Koderne skal skiftes regelmæssigt, være komplekse og være en minimumslængde, og hvis dette ikke er tilfældet, så inaktiveres medarbejderens bruger automatisk. Dette er gældende for medarbejdernes brugere, men også kundernes brugere i kundesystemer. Passwords på domænet er kontrolleret via regler defineret i GPO'er.

10. Kryptografi

Vi anvender som minimum 256 bit kryptering via VPN til kundesites og datacenter. Adgang udenfor godkendt netværk foregår via SSL-VPN og 2 faktor godkendelse.

11. Fysisk og miljømæssige sikringer

Fysisk skalsikring
Virksomheden har beliggenhed på grund planet af den bygning, hvor virksomheden er lokaliseret. Der er branddøre til hvert lokale.

Fysisk adgangskontrol
Ved tilstedeværelse af medarbejdere på kontoret er der fuld adgang for autoriserede og uautoriserede personer til alle lokaler med undtagelse af lageret. Lageret er beskyttet af en kodelås i alle 24 timer af døgnet. Nogle af lokalerne ligger uden for medarbejdernes periferi og synsfelt. Medarbejderne har nøgle til alle lokaler udover lageret, hvor det kun er autoriseret personale, der kan få adgang. Der følges ikke løbende op på hvilke personer, der har adgang til lageret, men det kontrolleres af CFO. Som udgangspunkt bliver eksterne personer, herunder leverandører og kunder, under besøg ledsaget af en medarbejder, men dette sker ikke i alle tilfælde. Ved medarbejder fravær er alle lokaler tilhørende C-SOLUTION ApS aflåst og kan kun tilgås af autoriseret personale og eksterne personer såsom rengøring.

Sikring af kontorer, lokaler og faciliteter
Alle lokaler er monteret med overvågningskamera og tyverialarm, hvoraf nogle af lokalerne også har røgkanoner. I tilfælde af indbrud alarmeres den private vagtcentral, og relevante personer i virksomheden alarmeres via app-notifikation. Adgang til vores faciliteter sker via numerisk tastatur og alarm applikation. Nogle lokaler aflåses, når medarbejder forlader lokalet, men det er ikke alle. Afhængig af antallet af medarbejdere, der er til stede, er dele af kontoret tilgængeligt for uvedkommende.

Udstyr

Brugerudstyr uden opsyn
Vi udfører awareness træning af medarbejderne omkring låsning af PC og password på mobiltelefoner.

Politik for ryddeligt skrivebord og blank skærm
Medarbejderne i C-SOLUTION ApS må ikke have følsomme oplysninger til at ligge på deres skriveborde.

12. Sikkerhed i forbindelse med drift

Dokumenterede driftsprocedurer
Vi har gennem vores IT driftspolitik faste processer for vores interne IT-drift, IT-drift af vores kunder og en beredskabsplan, herunder en eskalationstrappe internt og ekstern. Dertil arbejder vi med dobbeltroller på vores systemer for at sikre personuafhængighed og en ansvarsoversigt for gennemsigtighed i vores system-repertoire.

Ændringsstyring
Vi har i C-SOLUTION ApS kontroller på plads, der sikrer, at ændringer i driftspolitikken som minimum skal godkendes af vores IT-sikkerhedsgruppe. Ligeledes har vi implementeret et kategoriseringssystem, så ændringer i driftspolitikken følger fastlagte retningslinjer ift. om der er tale om småtilpasninger eller store ændringer. Store ændringer i driftspolitikken kræver godkendelse fra ledelsen.

Kapacitetsstyring
Vi har en fast rutine for kundeopfølgningsmøder, hvor vores kunder har mulighed for at tilkendegive et behov for kapacitetsændring. Derudover har kunderne selv mulighed for at kontakte os ved ekstraordinært behov for kapacitetsændring.

Adskillelse af udviklings-, test- og driftsfaciliteter
Vi har løsninger på plads, der sikrer vores kunders servere mod bl.a. adgang fra C-SOLUTION ApS' kontornetværk. Ligeledes er adgang til vores kunders servere beskyttet med VPN og 2-faktor godkendelse. Det er kun udvalgt personale, der har adgang til administrationen.

Beskyttelse mod malware
I C-SOLUTION ApS benyttes godkendte sikkerhedsforanstaltninger til at sikre mod eksterne skadevoldende handlinger herunder antivirus, mailfilter og firewall. Hertil har vi evalueringsværktøjer på plads til at revidere og godkende sikkerhedsløsninger målrettet at opnå den højest mulige sikkerhed ved at benytte markedsledende løsninger.

Backup

Sikkerhedskopiering af informationer
Vi tilbyder vores kunder at kunne genskabe deres systemer og data gennem backups på en hensigtsmæssig og korrekt måde understøttet af faste kontroller, der sikrer vores kunder den bedste løsning. Vi bruger troværdige underleverandører til backup, og disse underleverandører evalueres minimum årligt af vores IT-sikkerhedsgruppe for at sikre, at der leveres en tidssvarende og driftssikker backupløsning.

Vores backup as a service sikrer, at vores kunder har mulighed for at tilpasse frekvensen af backups efter eget behov og retention policy. Dette sikrer, sammen med high level support fra os, at vores kunder kan føle sig trygge omkring deres systemer og data.

Logning og overvågning

Hændelseslogning
Vi har opsat overvågning og logning af firewall gennem SCOM (System Center Operation Manager), der styres af vores driftsafdeling. SCOM er sat op, så driftsafdelingen får rettidige notifikationer om mistænkelige hændelser, der relaterer sig til forhold afdækket i log.

Beskyttelse af logoplysninger
Logs er sendt til en logningsdatabase, hvor det ikke er muligt hverken at ændre eller slette loggen. Dertil er selve loggen beskyttet jf. proceduren for adgangsstyring.

Administrator- og operatørlog
Logning af administratorer sker i forbindelse med den almindelige logning, og det er derfor heller ikke muligt at slette eller ændre loggens indhold.

Tidssynkronisering
Vi benytter offentlig NTP server til tidsstyring og benytter lokal server til tidssynkronisering afhængig af fysisk lokation.

Styring af software på driftssystemer

Installation af programmer på driftssystemer
Gennem vores IT driftspolitik har vi fastlagte retningslinjer, der sikrer, at vi følger en fast patch management cyklus. Denne suppleres af vores politik og regler for medarbejderrettigheder, så vi skaber gennemsigtighed I cyklussen og sikkerhed.

Styring af tekniske sårbarheder
For at holde os oplyste omkring sikkerhedssvagheder i de systemer og applikationer vi anvender internt og i kundeøjemed, afholder vores IT-sikkerhedsgruppe månedligt evalueringsmøde omkring generelle sårbarheder i de applikationer, hardwareløsninger m.m., der benyttes i C-SOLUTION ApS. Vores medarbejdere i IT-Drift og support holder dagligt øje med akut opståede sårbarheder og nyheder omkring de applikationer og hardwareløsninger, som C-SOLUTION ApS benytter sig af. I tilfælde af, at der opstår akutte kritiske sårbarheder, har vi fastlagte processer jf. vores driftspolitik der sikrer, at der bliver taget hånd om disse.

Begrænsning af programinstallering
Vi har procedurer på plads, der sikrer, at medarbejderne som udgangspunkt har de nødvendige programmer installeret på deres PC, samt at de får opdateringer til programmet. Da C-SOLUTION ApS' grundlag bygger på at videresælge underleverandørers løsninger, strider det imod vores forretningsmodel at begrænse installation af programmer. I stedet har vi politikker på plads, der sikrer, at de programmer, vi bruger, skal opfylde nogle sikkerhedsmæssige krav, som vores IT-sikkerhedsgruppe er ansvarlige for.

13. Kommunikationssikkerhed

Netværksforanstaltninger
IT-sikkerheden omkring systemers og datas ydre rammer er vores netværk mod internettet, remote og lignende. I C-SOLUTION ApS har vi foretaget de nødvendige sikkerhedsforanstaltninger, der sikrer imod uvedkommende adgang som er af højeste prioritet hos os. I C-SOLUTION ApS har vi faste rammer for vores netværk og netværkssikkerhed, hvorpå der er udarbejdet procedurer, vejledninger og dokumentation for driften og vedligehold af netværket.

Sikring af netværkstjenester
Adgangen til vores systemer fra vores kunder sker via det offentlige netværk igennem krypteret VPN-adgang. Derudover er det opsat en firewall i begge ender af VPN forbindelsen, hvorpå der er lavet regler for den tilladte trafik.

Opdeling af netværk
Det interne netværk er på lokationen segmenteret, således at det interne netværk er adskilt fra gæstenetværket.

Dataoverførsel

Politikker og procedurer for dataoverførsel
Ekstern datakommunikation sker alene via mails og Teams. Fortrolige informationer udveksles ikke via mails eller Teams til eksterne kunder. Førstegangskodeord til kundevendte eller interne systemer fremsendes via mails, men skal ændres ved første logon. Glemte kodeord, personoplysninger, bestillinger mv. håndteres via telefon og mail, og først efter at vores medarbejdere har konstateret, at det er den rigtige person, vi har kontakt til.

Elektroniske meddelelser
I C-SOLUTION ApS bruger vi e-mails til ekstern korrespondance samt Microsoft Teams til interne krypterede beskeder.

Fortrolighedsaftaler eller NDA (non-disclosure agreements)
Der er etableret fortrolighed generelt for alle involverede i vores forretning. Dette sker via ansættelseskontrakter eller samarbejdsaftaler med underleverandører og samarbejdspartnere.

15. Leverandørforhold

Informationssikkerhed i leverandørforhold
I C-SOLUTION ApS har vi formelle krav til de leverandører, vi indgår aftaler med i forhold til deres IT-sikkerhedspolitik, således at de IT-mæssige risici, der er forbundet med samarbejdet, minimeres.

Sikkerhedsforhold i leverandøraftaler
Vi sikrer, at IT-sikkerhedskrav er etableret og indgået med hver enkelt af vores leverandører ved at indskrive det i vores kontrakter. I vores leverandørforhold, der er etableret uden kontrakt, sammenholder vi periodisk deres informationssikkerhedspolitik med vores egne standarder.

Overvågning og evaluering af serviceydelser fra tredjeparter
Vi har kontroller på plads, der sikrer, at de leverandører, vi arbejder sammen med, har en godkendt revisorerklæring eller sikkerhedspolitikker, der lever op til vores egen standard eller højere.

Styring af ændringer af serviceydelser
Ved ændringer af vores politikker, procedurer eller kontroller foretages der altid en efterfølgende analyse af hvilke kunder og samarbejdspartnere, der bliver påvirket af ændringer. I de tilfælde hvor vores kunder eller samarbejdspartnere påvirkes, informeres disse rettidigt omkring ændringernes betydning for den konkrete aftale.

16. Styring af sikkerhedshændelser

Ansvar og procedurer
Vores medarbejdere er forpligtiget til at holde sig opdaterede vha. producenternes supporthjemmesider, debatfora mv. for konstaterede svagheder i de systemer, vi benytter og tilbyder.

Rapportering af informationssikkerhedshændelser
Vores supportafdeling, hvor vi håndterer langt de fleste sager for kunder og interne forhold, er samtidig vores system til håndtering af sikkerhedshændelser. Heri kan vi eskalere forhold således, at opgaver får højere prioritet end andre. Herudover vil sikkerhedshændelser afstedkommet fra hhv. egne observationer, alarmering ud fra log- og overvågningssystem, telefoniske henvendelser fra kunder, underleverandører eller samarbejdspartnere, blive eskaleret fra vores support til driftsafdelingen med samtidig orientering til ledelsen.

Rapportering af sikkerhedssvagheder
Vores medarbejdere og eksterne samarbejdspartnere er, via de indgåede kontrakter og aftaler, forpligtet til at anmelde enhver sikkerhedshændelse til nærmeste leder, så der hurtigst muligt kan reageres på hændelsen, og nødvendige tiltag kan udføres jf. etablerede procedurer.

Vurdering af informationssikkerhedsbrud
Gennem leverandørerne af benyttede software og hardware er der tilmeldt diverse e-mail lister samt platforme til indberetning, vurdering og eventuelle løsning, hvis et informationssikkerhedsbrud skulle blive opdaget.

Reaktion på informationssikkerhedshændelser
Ud fra de førnævnte platforme reageres der på informationssikkerhedshændelser på baggrund af hver enkelte tilfælde og producentens anbefalinger.

At lære af informationssikkerhedsbrud
Efter et informationssikkerhedsbrud laves der et debriefing møde, hvor hele forløbet gennemgås, samt hvilke erfaringer vi har gjort os.

17. Informationssikkerhedsaspekter ved beredskabsstyring

Beredskabsplanlægning
Vi har en formel og fast procedure på plads til styring af beredskabsplanlægning på alle niveauer.

Implementering af nødplaner og procedurer
Vi har fastlagte procedurer for beredskab, herunder en eskaleringsplan og vagtplan, der sikrer, at vi effektivt kan håndtere nødsituationer 24 timer i døgnet, 7 dage om ugen.

Prøvning, vedligeholdelse og revurdering af beredskabsplaner
Da vi ikke selv drifter noget, er vi afhængige af vores samarbejdspartnere og deres beredskabsplaner. Her kræver vi dog af vores samarbejdspartnere, at de som minimum tester deres beredskabsplan årligt, så vi sikrer, at vores kunder i mindst muligt omfang vil blive ramt i tilfælde af nødsituationer.

Redundance

Tilgængelighed af driftssystemer
Vi har etableret tilstrækkelig redundans for at imødegå krav til tilgængelighed.

18. Overensstemmelse

Uafhængig evaluering af informationssikkerhed
For at evaluere vores informationssikkerhed har vi etableret et samarbejde med en ekstern IT-revisor i forbindelse med udarbejdelse af de årlige ISAE 3402 erklæringer.

Overensstemmelse med sikkerhedspolitikker og sikkerhedsstandarder
For at sikre udførelse af IT-sikkerhedsaktiviteter til sikring af overensstemmelse med sikkerhedspolitikker og sikkerhedsstandarder har vi etableret et årshjul med de relevante aktiviteter.

Komplementerende kontroller

C-Solution ApS' kunder er, medmindre andet er aftalt, ansvarlige for at etablere forbindelse til servere, der vedligeholdes af C-Solution ApS' leverandører. Hertil er C-Solution ApS' kunder, medmindre andet er aftalt, ansvarlige for backup frekvens. Ligeledes er C-Solution ApS' kunder ansvarlige for:

- At det aftalte niveau for backup er dækkende
- At informere om behov for nedlæggelse eller oprettelse af kundens egne brugere efter kundens behov.
- At informere om behov for bestilling af nye aktiver.

Afsnit 2: C-SOLUTION ApS' udtalelse

Medfølgende beskrivelse er udarbejdet til brug for kunder, der har anvendt C-SOLUTION ApS' hosting-platform, og deres revisorer, som har en tilstrækkelig forståelse til at overveje beskrivelsen sammen med anden information, herunder information om kontroller, som kunderne selv har anvendt, ved vurdering af risiciene for væsentlig fejlinformation i kundernes regnskaber.

C-SOLUTION ApS anvender serviceunderleverandørerne Teamblue A/S og Cloud.factory A/S. Denne erklæring er udarbejdet efter partielmetoden, og C-SOLUTION ApS' kontrolbeskrivelse omfatter ikke kontrolmål og tilknyttede kontroller hos Teamblue A/S og Cloud.factory A/S. Enkelte af de kontrolmål, der er anført i C-SOLUTION ApS' beskrivelse i afsnit 1 af generelle IT-kontroller, kan kun nås, hvis de komplementerende kontroller hos kunderne er hensigtsmæssigt udformet og implementeret sammen med kontrollerne hos C-SOLUTION ApS. Erklæringen omfatter ikke hensigtsmæssigheden af udformningen og funktionaliteten af disses komplementerende kontroller.

C-SOLUTION ApS bekræfter, at:

(a) Den medfølgende beskrivelse i afsnit 1, giver en retvisende beskrivelse af de generelle it-kontroller med relevans for C-SOLUTION ApS' hosting-platform, der har behandlet kunders transaktioner pr. 27. januar 2022.

Kriterierne for denne udtalelse var, at den medfølgende beskrivelse:

(i) Redegør for, hvordan kontrollerne har været udformet og implementeret, herunder redegør for:
- De typer af ydelser, der er leveret.
- De processer i både it- og manuelle systemer, der er anvendt til styring af de generelle it-kontroller.
- Relevante kontrolmål og kontroller udformet til at nå disse mål.
- Kontroller, som vi med henvisning til kontrollernes udformning har forudsat ville være implementerede af brugervirksomheder, og som, hvis det er nødvendigt for at nå de kontrolmål, der er anført i beskrivelsen, er identificeret i beskrivelsen sammen med de specifikke kontrolmål, som vi ikke selv kan nå.
- Andre aspekter ved vores kontrolmiljø, risikovurderingsproces, informationssystem og kommunikation, kontrolaktiviteter og overvågningskontroller, som har været relevante for de generelle it-kontroller.

(ii) Indeholder relevante oplysninger om ændringer i de generelle it-kontroller foretaget pr. 27. januar 2022

(iii) Ikke udelader eller forvansker oplysninger, der er relevante for omfanget af det beskrevne system under hensyntagen til, at beskrivelsen er udarbejdet for at opfylde de almindelige behov hos en bred kreds af kunder og deres revisorer og derfor ikke kan omfatte ethvert aspekt ved systemet, som den enkelte kunde måtte anse vigtigt efter deres særlige forhold.

(b) De kontroller, der knytter sig til de kontrolmål, der er anført i medfølgende beskrivelse, var hensigtsmæssigt udformede og implementeret pr. 27. januar 2022.

Kriterierne for denne udtalelse var, at:

(i) De risici, der truede opnåelsen af de kontrolmål, der er anført i beskrivelsen, var identificeret

(ii) De identificerede kontroller ville, hvis anvendt som beskrevet, give høj grad af sikkerhed for, at de pågældende risici ikke forhindrede opnåelsen af de anførte kontrolmål.

Horsens, den 9. februar 2022
C-SOLUTION ApS

Brian Pedersen

Brian Pedersen
Adm. Direktør

Afsnit 3: Uafhængig revisors erklæring om beskrivelsen af kontroller, deres udformning og implementering

Til C-SOLUTION ApS, deres kunder, og deres revisorer.

Omfang

Vi har fået til opgave at afgive erklæring om C-SOLUTION ApS' beskrivelse i afsnit 1 af generelle it-kontroller for drift af hostingydelser og om udformningen og implementering af kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

Vi har ikke udført handlinger vedrørende funktionaliteten af de kontroller, der indgår i beskrivelsen, og udtrykker derfor ingen konklusion herom.

C-SOLUTION ApS anvender serviceunderleverandørerne Teamblue A/S og Cloud.factory A/S. Denne erklæring er udarbejdet efter partielmetoden, og C-SOLUTION ApS' kontrolbeskrivelse omfatter ikke kontrolmål og tilknyttede kontroller hos Teamblue A/S og Cloud.factory A/S.

Enkelte af de kontrolmål, der er anført i C-SOLUTION ApS' beskrivelse i afsnit 1 af generelle it-kontroller, kan kun nås, hvis de komplementerende kontroller hos kunderne er hensigtsmæssigt udformet og implementeret sammen med kontrollerne hos C-SOLUTION ApS. Erklæringen omfatter ikke hensigtsmæssigheden af udformningen og funktionaliteten af disses komplementerende kontroller.

C-SOLUTION ApS' ansvar

C-SOLUTION ApS er ansvarlig for udarbejdelsen af beskrivelsen (afsnit 1) og tilhørende udtalelse (afsnit 2), herunder fuldstændigheden, nøjagtigheden og måden, hvorpå beskrivelsen og udtalelsen er præsenteret; for leveringen af de ydelser, beskrivelsen omfatter, for at anføre kontrolmålene samt for udformningen og implementeringen af fungerende kontroller for at nå de anførte kontrolmål.

REVI-IT A/S' uafhængighed og kvalitetsstyring

Vi har overholdt kravene til uafhængighed og andre etiske krav i International Ethics Standards Board for Accountants' internationale retningslinjer for revisorers etiske adfærd (IESBA Code), der bygger på de grundlæggende principper om integritet, objektivitet, professionel kompetence og fornøden omhu, fortrolighed og professionel adfærd, samt etiske krav gældende i Danmark.

REVI-IT anvender ISQC 1[1] og opretholder derfor et omfattende system for kvalitetsstyring, herunder dokumenterede politikker og procedurer for overholdelse af etiske regler, faglige standarder samt gældende krav ifølge lov og øvrig regulering.

[1] ISQC 1, Kvalitetsstyring i firmaer, som udfører revision og review af regnskaber, andre erklæringsopgaver med sikkerhed og beslægtede opgaver.

REVI-IT A/S' ansvar

Vores ansvar er på grundlag af vores handlinger at udtrykke en konklusion om C-SOLUTION ApS' beskrivelse (afsnit 1) og om udformningen og implementeringen af kontroller, der knytter sig til de kontrolmål, der er anført i denne beskrivelse. Vi har udført vores arbejde i overensstemmelse med ISAE 3402, "Erklæringer med sikkerhed om kontroller hos en serviceleverandør", som er udstedt af IAASB og yderligere krav ifølge dansk revisorlovgivning.

Denne standard kræver, at vi planlægger og udfører vores handlinger for at opnå en høj grad af sikkerhed for, at beskrivelsen i alle væsentlige henseender er retvisende, og at kontrollerne i alle væsentlige henseender er hensigtsmæssigt udformede og implementeret.

En erklæringsopgave med sikkerhed om at afgive erklæring om beskrivelsen, udformningen og implementeringen af kontroller hos en serviceleverandør omfatter udførelse af handlinger for at opnå bevis for oplysningerne i serviceleverandørens beskrivelse af sit system og for kontrollernes udformning. De valgte handlinger afhænger af serviceleverandørens revisors vurdering, herunder vurderingen af risiciene for, at beskrivelsen ikke er retvisende, og at kontrollerne ikke er hensigtsmæssigt udformet eller implementeret.

En erklæringsopgave med sikkerhed af denne type omfatter desuden en vurdering af den samlede præsentation af beskrivelsen, hensigtsmæssigheden af de heri anførte mål samt hensigtsmæssigheden af de kriterier, som serviceleverandøren har specificeret og beskrevet C-SOLUTION ApS' udtalelse i afsnit 2.

Det er vores opfattelse, at det opnåede bevis er tilstrækkeligt og egnet til at danne grundlag for vores konklusion.

Begrænsninger i kontroller hos en serviceleverandør

C-SOLUTION ApS' beskrivelse i afsnit 1 er udarbejdet for at opfylde de almindelige behov hos en bred kreds af kunder og deres revisorer og omfatter derfor ikke nødvendigvis alle de aspekter ved de generelle it-kontroller, som hver enkelt kunde måtte anse for vigtigt efter deres særlige forhold. Endvidere vil kontroller hos en serviceleverandør som følge af deres art muligvis ikke forhindre eller afdække alle fejl eller udeladelser ved behandlingen eller rapporteringen af transaktioner.

Konklusion

Vores konklusion er udformet på grundlag af de forhold, der er redegjort for i denne erklæring. De kriterier, vi har anvendt ved udformningen af konklusionen, er de kriterier, der er beskrevet i C-SOLUTION ApS' udtalelse i afsnit 2. Det er vores opfattelse, at:

(a) Beskrivelsen af de generelle it-kontroller, således som de var udformet og implementeret pr. 27. januar 2022, i alle væsentlige henseender er retvisende
(b) Kontrollerne, som knytter sig til de kontrolmål, der er anført i beskrivelsen, i alle væsentlige henseender var hensigtsmæssigt udformet pr. 27. januar 2022

Tiltænkte brugere og formål

Denne erklæring er udelukkende tiltænkt kunder, der har anvendt C-SOLUTION ApS' hosting-platform, og deres revisorer, som har en tilstrækkelig forståelse til at overveje den sammen med anden information, herunder information om kunders egne kontroller, når de vurderer risiciene for væsentlige fejlinformationer i deres regnskaber.

København, den 9. februar 2022

REVI-IT A/S
Statsautoriseret revisionsaktieselskab

Henrik Paaske
Statsautoriseret revisor

Christian H. Riis
Partner, CISA,