

Wannafind

Erklæring fra uafhængig revisor vedrørende generelle it-kontroller i Wannafind

Marts 2010

Wannafind
Att.: Jakob Schwartz
Sverigesvej 8
8660 Skanderborg

Erklæring fra uafhængig revisor vedrørende design og implementering af generelle it-kontroller pr. 26. februar 2010

Indledning

Wannafind tilbyder sine kunder en række forskellige ydelser inden for outsourcingaktiviteter omkring WEBHoteller, hostede applikationer/services, udlejning af servere og Co location ydelser.

Vi har indgået en aftale med Wannafind om at påse, at Wannafind efterlever selskabets egen it-sikkerhedspolitik i relation til outsourcingsaktiviteterne. Nærværende dokument er således en erklæring om, at forretningsgange og procedurer er tilrettelagt i overensstemmelse med det anførte i sikkerhedspolitikken. Revisionen tager udgangspunkt i it-sikkerhedspolitik version 2.3. af 26. februar 2010, og de kontroller som selskabet har implementeret til at efterleve it-sikkerhedspolitikken.

Det er ledelsens ansvar at etablere og sikre kontroller til efterlevelse af it-sikkerhedspolitikken. Vores ansvar er, baseret på vores arbejde, at udtrykke en konklusion om, hvorvidt vi enig i, at selskabet har designet og implementeret kontroller, som sikre, at it-sikkerhedspolitikken efterleves.

Vores erklæring er udarbejdet til brug for Wannafind og de af Wannafinds kunder, som enten har eller ønsker at indgå aftale med Wannafind om varetagelse af it-drift og it-serviceydelser samt disses revisorer.

Den udførte revision

Vores arbejde er udført i overensstemmelse med den danske revisionsstandard om it-erklæringer (RS3411 – type A) med henblik på at opnå høj, men ikke fuldstændig grad af sikkerhed for vores konklusion omkring, at selskabet har tilrettelagt og implementeret betryggende generelle it-kontroller. Vores revision har ikke omfattet en test af de generelle it-kontrollers effektivitet, og gennemgangen er således alene udtryk for, om der forefindes betryggende kontroller pr. den 26. februar 2010, men ikke hvorvidt disse har været opretholdt over en periode.

Revisionen omfatter forespørgsler, observationer samt vurdering og stikprøvevis efterprøvelse af den information, vi har modtaget. Det er vores opfattelse, at det udførte arbejde giver et tilstrækkeligt grundlag for vor konklusion.

På grund af begrænsninger i ethvert kontrolsystem kan der opstå fejl eller besvigelser, som ikke af-dækkes af vores arbejde. Endvidere vil en anvendelse af vores konklusion omkring betryggende tilret-telæggelse og implementering på efterfølgende perioder være undergivet en risiko for, at der foretages ændringer af systemer eller kontroller, ændring i kravene til behandling af oplysninger eller Wanna-find overholdelse af de beskrevne politikker og procedurer, hvorved vores konklusion eventuelt ikke længere vil være gældende.

I vedlagte bilag 1 har vi anført de kontrolområder, som er omfattet af erklæringen samt vores bemærk-ninger til de enkelte kontrolområder.

Konklusion

Det er vores opfattelse, at generelle it-kontroller hos Wannafind til efterlevelse af it-sikkerhedspolitik version 2.3 af 26. februar 2010 er hensigtsmæssigt designet og implementeret.

Århus, den 12. marts 2010

Deloitte

Statsautoriseret Revisionsaktieselskab



Mikkel Schøning
statsautoriseret revisor, CISA

Bilag 1: Kontrolområder

Nedenfor vises Deloitte's kontrolområder og –aktiviteter for generelle it-kontroller.

Kontrolområder
Fysisk sikkerhed
Miljø og sikring <ul style="list-style-type: none">- Datacenteret er beskyttet med udstyr der kendetegner et professionelt hostingmiljø, herunder sikring af køling, brandsikring, sikring mod oversvømmelse samt sikring af strøm og nødstrøm.
Adgangskontrol <ul style="list-style-type: none">- Det er udelukkende clearede driftsteknikere der har adgang til datacenteret, herunder procedurer for adgang til eksterne personer, videoovervågning og kontroller til sikring mod indbrud og sabotage.
Hardware
Redundansniveau <ul style="list-style-type: none">- Procedurer og krav til opbygning af redundante.
Spareparts og udskiftning <ul style="list-style-type: none">- Procedurer og krav til opbevaring af reservedele, herunder procedurer for valg af stabile leverandører og etablering af support på hardware til hostingcenteret.
Datasikkerhed
Brugte lagermedier <ul style="list-style-type: none">- Procedurer og krav til sikker destruktion af lagermedier.
Sikkerhedskopiering/backup <ul style="list-style-type: none">- Procedurer for sikkerhedskopiering og backup, herunder styring, opbevaring og re-etablering af systemer og data. Revisionen omfatter også en vurdering af de fysiske elementer i forbindelse med opbevaring af backups.
Antivirus <ul style="list-style-type: none">- Procedurer for installation og overvågning af antivirus på interne management systemer.
Logisk sikkerhed
Adgangskoder <ul style="list-style-type: none">- Procedurer og krav omkring anvendelse af password på systemer og til data ud fra den enkelte medarbejders arbejdsbetinget behov for adgang.
Overvågning og rapportering <ul style="list-style-type: none">- Procedurer og krav til etableret overvågning dels på fysiske forhold som serverrum og aktivt udstyr og dels på services på de hostede systemer.

Kontrolområder
Vagtprocedurer <ul style="list-style-type: none"> - Procedurer og krav til sikring af en betryggende vagtordning. - Procedurer og krav til efterlevelse af reaktionstider i forbindelse med vagtordning.
Driftsudmeldninger <ul style="list-style-type: none"> - Procedurer og krav til regelmæssig vedligeholdelse af udstyr, herunder information til kunderne samt placering af servicevinduer.
Netværk
Netværksdiagram <ul style="list-style-type: none"> - Procedurer og krav til netværksdokumentation samt opdatering af disse.
Dokumentation
Teknisk dokumentation <ul style="list-style-type: none"> - Procedurer og krav til netværksdokumentation samt opdatering af disse.
Procedurer <ul style="list-style-type: none"> - Krav og formelle procedurer på alle kritiske driftsoperationer, herunder nødprocedurer for uplanlagte systemnedbrud. - Krav til/om tilkaldelse af eksterne eksperter.