Uafhængig revisors erklæring med sikkerhed om
beskrivelsen af kontroller og deres udformning
i forbindelse med udvikling og drift af softwaren Hero Outbound
pr. 1. september 2018

ISAE 3402, type I

HeroBase A/S

CVR-nr. 31 07 31 03

September 2018

Indholdsfortegnelse

Afsnit 1: HeroBase A/S' udtalelse

Medfølgende beskrivelse er udarbejdet til brug for kunder, der har anvendt HeroBase A/S' driftsydelser i forhold til ydelsen Hero Outbound, 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. HeroBase A/S bekræfter, at:

(a) Den medfølgende beskrivelse, i afsnit 2, giver en retvisende beskrivelse af HeroBase A/S' udvikling og drift af softwaren Hero Outbound til kunder pr. 1. september 2018. Kriterierne for denne udtalelse var, at den medfølgende beskrivelse:

(i) Redegør for, hvordan systemet var udformet og implementeret, herunder redegør for:

- De typer af ydelser, der er leveret, når det er relevant
- De processer i både it- og manuelle systemer, der er anvendt til at igangsætte, registrere, behandle og om nødvendigt korrigere transaktionerne samt overføre disse til de rapporter, der er udarbejdet til kunder
- Relevante kontrolmål og kontroller, udformet til at nå disse mål
- Kontroller, som vi med henvisning til systemets udformning har forudsat ville være implementeret af brugervirksomheder, og som, hvis det er nødvendigt for at nå de kontrolmål, der er anført i beskrivelsen, er identificerede 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 behandlingen og rapporteringen af kunders transaktioner.

(ii) 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 fungerede effektivt pr. 1. september 2018. Kriterierne for denne udtalelse var, at:

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

(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.

Søborg, 1. september 2018

HeroBase A/S

Casper Langhoff
Adm. direktør

Kenny Andreasen
CTO & CIO

Afsnit 2: HeroBase A/S' beskrivelse af udvikling og drift af softwaren Hero Outbound samt interne kontroller

Introduktion

Formålet med denne beskrivelse er at levere information til HeroBases kunder og deres interessenter (herunder revisorer) vedrørende kravene i den internationale revisionsstandard for erklæringsopgaver om kontroller hos en serviceleverandør, ISAE3402.

Beskrivelsen har herudover det formål at give information om vores informationssikkerhedsregelsæt, procedurer og kontroller, som er gældende for vores leverance af produktet og ydelsen Hero Outbound til vores kunder.

Beskrivelsen omfatter de kontrolmål og kontroller vedrørende Hero Outbound, som omfatter størstedelen af vores kunder og er baseret på vores standardleverance. Individuelle kundeforhold er ikke medtaget i denne beskrivelse.

HeroBase og vores software Hero Outbound

HeroBase er en dansk IT-virksomhed med base i Søborg. Vi udvikler, hoster og leverer software til kontaktcentre som en SaaS-løsning. Vores kerneprodukt er leverance af softwaren Hero Outbound, der leveres som SaaS-løsning, dvs. er hostet i egne datacentre og bygget op omkring en fleksibel og skalérbar abonnementsbaseret model.

Hero Outbound, som denne erklæring går på, er i øjeblikket det største produkt i vores palette af løsninger samlet under Hero-brandet. Andre løsninger indbefatter bl.a. marketing automation platformen Hero Flows, og rådgivnings- og salgstræningsorganet Hero Academy. Hero er valgt som paraplybetegnelse, fordi vi med vores løsninger gerne vil appellere direkte til slutbrugerne af vores software; for Hero Outbounds vedkommende betyder det mestendels brugerne og medarbejderne – også kaldet agenterne – i kontaktcentre – også kaldet callcentre. Vi vil ved at levere en hurtig, intuitiv, effektiv og personlig platform være det foretrukne valg blandt "hverdagens helte", som agenterne i kontaktcentrene omtales som internt i HeroBase.

Vi skaber fundamentet for det mest effektive kontaktcenter

Navnet Hero Outbound er valgt til den løsning, som i øjeblikket er den bærende, fordi den først og fremmest fokuserer på opsøgende salg/rådgivningsarbejde, også kaldet outbound telemarketing. Telemarketing er, om end termen til tider behæftes med en negativ association, fortsat en uhyre effektiv kontaktkanal, fordi den giver mulighed for at dyrke den personlige kontakt mellem agent og personen i "den anden ende af røret". Salgs- og kundekontakter, som starter med opsøgende salg, er dog ingenlunde afgrænset til outbound telemarketing alene. E-mails og SMS'er ligger i naturlig forlængelse af den telefoniske dialog – enten i forbindelse med digital ordreaccept, udsendelse af opfølgende information, koordinationsarbejde o. lign. Hero Outbound muliggør tillige at indgående telefonopkald besvares "blandet" med de udgående telefonopkald – typisk når der ringes tilbage fra personer, som har et ubesvaret opkald på deres telefon, eller i forbindelse med indgående salgshenvendelser affødt af kampagner o. lign.

Hero Outbound kan således, selv uden produkter fra den øvrige palette af Hero-løsninger, for mange kontaktcentre udgøre den eneste nødvendige software, centret skal bruge til at udføre sine aktiviteter blandt agenterne (salg, mødebooking, fundraising, meningsmålinger o.m.a.) og blandt ledere og administratorer, som tilrettelægger og monitorerer agenternes arbejde.

Disse ”aktiviteter” indbefatter også selve handlingen at ringe ud eller besvare telefonen. Som webapplikation betjenes Hero Outbound fra en browser, og med et headset tilsluttet til computeren kan telefonopkald udføres og besvares via den indbyggede samtaleteknologi Hero Phone, som er baseret på WebRTC-frameworket. Hermed er ingen eksterne telefoner eller tredjepartsløsninger nødvendige for at gennemføre kontaktaktiviteterne. Ønskes det at ringe via en eksisterende telefon som findes på arbejdsstationen – f.eks. en SIP-telefon eller fastnettelefon installeret af virksomheden – kan denne også bruges sammen med Hero Outbound, idet applikation kan forbinde til en ekstern telefon og holde linjen åben, hvormed der forbindes og tales via den eksterne telefon.

Et centralt system blandt andre forretningssystemer

På integrationssiden tilbyder Hero Outbound en række muligheder for at integrere med andre løsninger for så vidt angår data ind og ud af platformen; brugeroprettelse; dokumentation af telefonopkald o.m.a. Hero Outbound har et veludbygget API, som kunder kan benytte uden meromkostning. Dette REST-API tillader adgang til kundens Hero Outbound-data ud fra rettigheder på funktions- og projektniveau, som defineres af kunden selv, og muliggør at hente, opdatere og slette logiske entiteter. Hvis kunden i højere grad ønsker data pushet fra Hero Outbound til eksterne systemer, i stedet for at pulle data fra vores REST-API, har platformen indbyggede ”triggers” – en slags webhooks – hvor regler kan opsættes til at udføre bestemte handlinger når bestemte ting er forekommende i systemet. Handlinger omfatter blandt andet kald til eksterne SOAP- eller REST-API’er, hvormed man kan integrere Hero Outbound med alle andre systemer uden at skrive en eneste linje kode – så længe man har et API, som kan kaldes fra Heros web-servere (et afgrænset IP-range) med enten XML eller JSON-objekter.

Ovenstående er en overordnet beskrivelse af Hero Outbound og en kort beskrivelse af nogle af de værktøjer, platformen stiller til rådighed. HeroBase ønsker med kunderne på Hero Outbound en langvarig kunderelation, hvor kunden over tid sammen med sin customer experience manager får taget større og større dele af platformen i brug, og hvor Hero Outbound integreres til andre nøglesystemer i kundens forretning. Dette tror vi muliggør sig gennem en teknisk stærk og stabil platform, hvor sikkerhed og performance er i højsædet, med et engageret teknisk og kundefokuseret team omkring sig.

Teknisk opbygning og placering

Hero Outbound er en webapplikation baseret på .NET (primært sprog er C#), med frontend baseret på bl.a. JavaScript, Angular og REACT. Databaseteknologi er MySQL, og hosting sker i de danske datacentre Global Connect (Taastrup) og InterXion (Ballerup). I skrivende stund er større dele af AWS’ (Amazon Web Services) løsninger ved at blive taget i brug. I første omgang med opbevaring af filer i S3 i stedet for på virtuelle servere i Danmark. Senere også med henblik på at have databaser i AWS’ Aurora. De eneste AWS-lokationer, vi har valgt services i og som data dermed forefindes i, er AWS’ Dublin-site i Irland samt AWS’ site i Frankfurt, og der er således intet data i Hero Outbound, som forlader EU. På telefoni-siden er ringning drevet af fysiske Linux-servere med Freeswitch som teleoperativsystem ovenpå. Vores infrastruktur og arkitektur er designet således at der findes redundant failover-udstyr til alt fra firewalls og switche til database- og teleservere. Det meste udstyr forefindes også i begge datacentre, således at en lokation kan tage over, hvis en anden lokation lider under nedsat fremkommelighed eller andre problematiske forhold, interne såvel som eksterne.

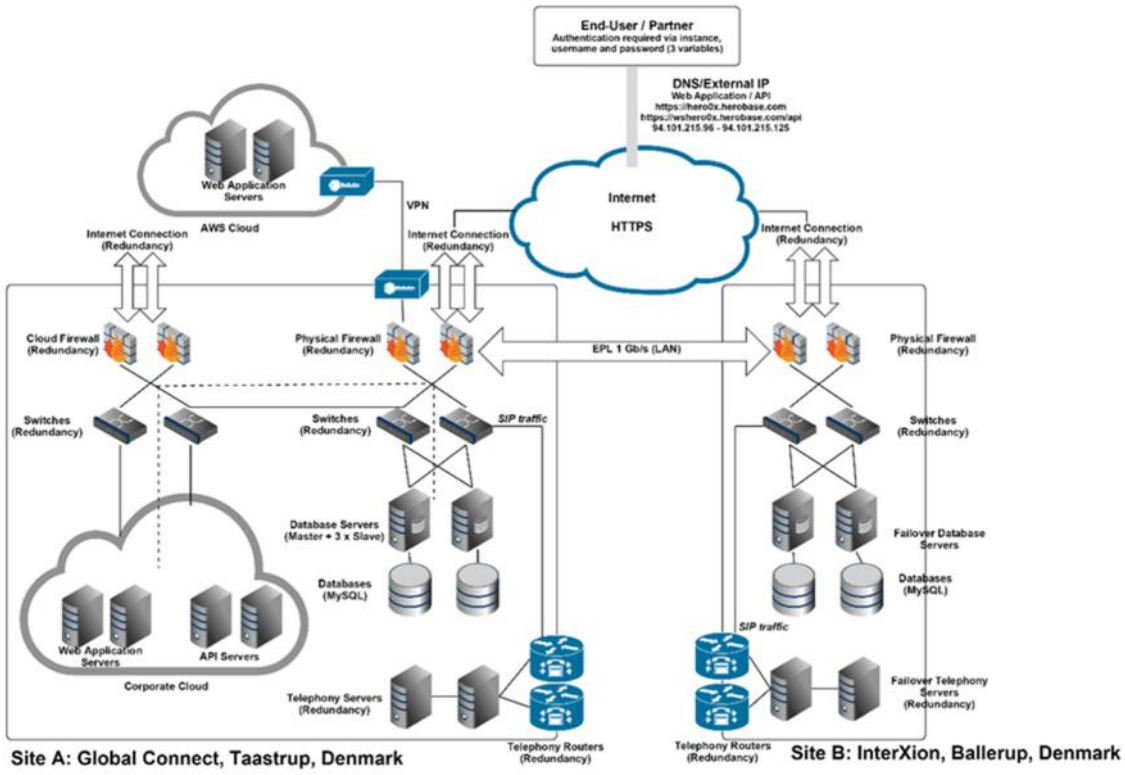

Fig. 1: Hero Outbound platformen, overordnet infrastruktur pr. medio 2018.

Vi tror på at appellere til hverdagens helte ved at designe komplette løsninger til deres arbejdspladser, og levere løsninger som gør kontaktcentre til konkurrencedygtige og effektive virksomheder ved at optimere arbejdstiden og rentabiliteten på centrenes opgaver, samtidig med at vi tilpasser platformen til nye eksterne krav såsom nye krav til betalingsløsninger, aftaledokumentation, GDPR o. lign. Vi tror på, at vi har Nordeuropas bedste software til branchen, og har internationale vækstmål baseret på et sundt og solidt hjemmemarked, hvor den gode daglige kontakt og langvarige kunderelation er i fokus!

Organisation og ansvar

HeroBase beskæftiger 30 medarbejdere i Danmark, Sverige, Ukraine, Spanien og Litauen. Godt halvdelen af medarbejderne er placeret i Danmark, og har daglig arbejdsplads på kontoret i Søborg.

Ledelsen består af en øverst ansvarlig CEO, og under ham en CTO med al teknisk ansvar samt en CXO med ansvar for kundekontakt, kunderelationer og support. Hertil en stabsfunktion med CFO samt administration og HR.

IT-afdelingen, som ledes af HeroBases CTO, består primært af udviklere i en "devops"-konstellation, hvor to mand er dedikeret til drift, optimering af servere og infrastruktur, overvågning og håndtering af operationelle issues, men hvor alle har drift som førsteprioritet i tilfælde af tekniske problemer på platformen. Det er en målsætning at egentlig udvikling, forstået som forbedring af eksisterende features og udvikling af nye, udgør 80% af afdelingens tid. Udviklerne er organiseret i frontend- og backend-ekspertiser, med en chefarkitekt som tager de overordnede beslutninger om sprog, teknologi og nye frameworks efter grundig analyse og i samarbejde med HeroBases CTO. Herudover er en netværksadministrator ansvarlig for netværk og telefoni, mens en projektleder og tester har et tæt samarbejde med HeroBases øvrige afdelinger.

Ledelsen er overordnet ansvarlig for IT-sikkerhed, og for at virksomhedens overordnede IT-sikkerhedspolitik overholdes.

Ved siden af den daglige funktionsopdelte organisation er der organiseret en sikkerhedsorganisation, med et informationssikkerhedsudvalg bestående af nøglemedarbejdere fra forskellige dele af HeroBase inkl. ledelsen, samt en informationssikkerhedskoordinator som har det daglige, operationelle ansvar for en række opgaver defineret i HeroBases informationssikkerhedsregelsæt. Informationssikkerhedskoordinatoren er desuden ansvarlig for at alle medarbejdere kender til informationssikkerhedshåndbogen, herunder regler og procedurer, hjælper dem med at tilgå og forstå den samt udleve og overholde reglerne. Slutteligt er ansvar for en række forhold omhandlende de forretningssystemer, som understøtter det daglige arbejde med at levere produktet og ydelsen Hero Outbound, uddelt til systemejerne.

Risikostyring i HeroBase A/S

Risikostyring i HeroBase A/S udføres inden for alle de områder, som har med leverancen af produktet og ydelsen Hero Outbound at gøre, og som dermed kan have en økonomisk konsekvens for vores kunder. Risikoanalyse, -vurdering og -styring er baseret på ISO27005, og tager udgangspunkt i konsekvensanalyser og sårbarhedsanalyser på serviceniveau. Service forstås som forretningssystemer som understøtter leverancen af Hero Outbound, samt selve Hero Outbound som kundesystem.

Forretningen i HeroBase svarer på konsekvensanalysens spørgsmål, mens IT-afdelingen i HeroBase gennemfører sårbarhedsanalyser. Sårbarhedsanalyser afrapporteres på serviceniveau, men tager udgangspunkt i aktiver, som er de fysiske og virtuelle delementer, som tilsammen udgør platformene eller forretningssystemerne. Eksempelvis er til servicen Hero Outbound en række afhængende aktiver som firewalls; switche; teleroutere; webapplikationsservere; databaseservere; telefoniservere m.v. Når afrapportering sker på serviceniveau, er det også klart at det er "laveste fællesnævner" som definerer f.eks. maksimalt mulige nedetid. Hvis en databaseserver altid vil kunne overtages af en failover-makker efter boot og DNS-skifte på 5 minutter, men det i yderste teori kan tage 15 minutter før en fysisk firewall vil være udskiftet med en bootet og konfigurationsindlæst redundant makker, er det klart at det er de 15 minutter, som vil definere den mulige nedetid.

Risikoanalyser gennemføres som konsekvens- og sårbarhedsanalyser mindst årligt, hvorefter det samlede sikkerhedsbillede bringes op for informationssikkerhedsudvalget og slutteligt HeroBases ledelse, til definition af nærmere handlinger.

Generelt om vores kontrolmål, herunder regler og procedurer, og implementerede kontroller

Det væsentligste i leverancen af produktet og ydelsen Hero Outbound er en stabil og sikker platform. Det er et erklæret og ledelsesforankret løfte at vi hellere vil bruge dobbelt så lang tid på at løse en udviklingsopgave eller anden teknisk opgave, end den kunne være løst på, for at sikre sikkerhed og stabilitet, når vi frigiver opdateringer til vores kunder.

For at leverancekæden kan fungere, og HeroBase samtidig kan fungere som konkurrencedygtig forretning herunder at opnå skalerbarhed over tid, er arbejdsgange og processer forbundet med levering af produktet og ydelsen Hero Outbound bygget op omkring vores informationssikkerhedsregelsæt, på toppen af hvilket der er defineret procedurer og kontroller med tilhørende beredskabsplaner m.m.

Aller øverst står vores top level information security policy, som er underskrevet af HeroBases CEO og sætter rammerne for arbejdet med informationssikkerhed. Denne gælder alle medarbejdere og nærtstående samarbejdspartnere (f.eks. konsulenter).

Referencerammen for informationssikkerhedsregelsættet er ISO27001, og regelsættet er derfor overordnet inddelt i følgende kontrolområder:

- Styring af informationssikkerhed og sikkerhedspolitik
- Organisering af informationssikkerhed
- Personalesikkerhed
- Styring af aktiver
- Adgangsstyring
- Kryptografi
- Fysisk sikring og miljøsikring
- Driftssikkerhed
- Kommunikationssikkerhed
- Anskaffelse, udvikling og vedligeholdelse af systemer
- Leverandørforhold
- Styring af informationssikkerhedsbrud og -hændelser
- Informationssikkerhedsaspekter ved nød-, beredskabs- og reetableringsstyring
- Overensstemmelse

Vi har desuden tilvalgt en række procedurer og politikker inden for rammerne af datasikkerhed og GDPR, og tager vores ansvar som databehandler for nogle af landets største virksomheder ekstremt seriøst. Op til effektueringen af GDPR har vi udvidet vores platform med en række features, som gør det nemmere for vores kunder som dataansvarlige at leve op til de krav, de bliver stillet af bl.a. GDPR. Vi vil gerne anses som datamedansvarlige i højere grad end som databehandler, og udtaler os gerne om dette i forskellige sammenhænge. Som databehandler har vi desuden sikret at vi har en databehandleraftale med alle vores kunder på Hero Outbound, som i denne konstellation er dataansvarlige.

Styring af informationssikkerhed og sikkerhedspolitik

HeroBases overordnede informationssikkerhedspolitik er udarbejdet med det formål at sikre en løbende forankring af arbejdsmetodikker, principper og rutiner, som lever op til det fastlagte sikkerhedsniveau.

Ledelsen godkender politikken som underskrives af vores CEO, og ledelsen er ansvarlig for at politikken overholdes.

Informationssikkerhedspolitikken skal overholdes i alle henseender og har til formål at sikre en sikker og stabil leverance af produktet og ydelsen Hero Outbound, herunder at relevant lovgivning overholdes, at alle væsentlige risici for driftsafbrydelser og datatyveri og -læk reduceres.

Politikken revideres og godkendes hvert år. Informationssikkerhedskoordinatoren er ledelsens og informationssikkerhedsudvalgets "forlængede arm" i den daglige forankring af politikken, og denne sikrer den løbende kommunikation til alle relevante parter. Alle medarbejdere underskriver desuden årligt at de har læst og efterlever politikken og den tilhørende informationssikkerhedshåndbog.

Organisering af informationssikkerhed

Funktionsadskillelse

Vi har en klar og veldefineret organisation, med funktionsadskillelse som gør at afhængighed af nøglepersoner er reduceret mest muligt. Der er desuden indført funktionsadskillelse på områder, hvor der er risiko for at der kan forekomme misbrug af virksomhedens data og informationer.

Kontakt med myndigheder

Vi har defineret ansvar for kontakt til offentlige myndigheder vedrørende emner inden for informationssikkerhedsområdet.

Projektstyring

Vi har defineret ansvar for, at HeroBases projektledelsesmodel på tilstrækkelig vis håndterer informationssikkerhed i alle faser, således at projekter ikke påvirker HeroBases risikobillede i negativ grad. Der tages stilling til informationssikkerhed i alle projekter, uanset deres størrelse.

Udstyr og fjernarbejdspladser

Vi har en procedure for anvendelse af mobilt udstyr og hjemmearbejdspladser/fjernarbejdspladser. Der er defineret minimumskrav for alle enheders beskyttelse, samt adgang til forretningssystemer og data. Alle enheder skal være beskyttet af antivirus og firewall. En række systemadgange til HeroBases forretningssystemer kræver VPN-adgang. Disse udstedes og installeres af HeroBases IT-afdeling (godkendelse af HeroBases CTO, udstedelse og opsætning af en medarbejder i IT-afdelingen). VPN kan installeres på PC'er udleveret og ejet af HeroBase, men aldrig på privat ejede PC'er.

Personalesikkerhed

Vi har defineret en række procedurer som sikrer sikkerhed før, under og evt. efter ansættelsen.

Procedurer som omhandler processer før en evt. ansættelse sikrer, at potentielle medarbejdere screenes og at relevante forhold kontrolleres inden for rammerne af gældende lovgivning.

Alle medarbejdere skal leve op til en række vilkår om fortrolighed om egne, HeroBases og kunders forhold. Dette er beskrevet i ansættelseskontrakten for hver medarbejder.

Under ansættelsen sikres det sammen med medarbejderen, nærmeste leder og informationssikkerhedskoordinatoren, at medarbejderen holdes ajour indenfor og efterleverer aspekter vedrørende informationssikkerhed.

Vi har procedurer som sikrer at medarbejdere ved ansættelsesophør ikke kan forvolde HeroBase eller systemet Hero Outbound skade, ved øjeblikkeligt at fjerne rettigheder til forretningssystemer og kontrollere dette.

Der er desuden defineret en række sanktioner såfremt informationssikkerheden overtrædes eller tilsidesættes.

Styring af aktiver

Alle aktiver er defineret med ejerskab, kritikalitet og tekniske afhængigheder som services, der afhænger af enkelte aktiver. Servere, systemer, netværk mv. er dokumenteret og til rådighed for relevant teknisk personale. Ved introduktion af nyt udstyr og nye systemer, eller ved ændringer i arkitekturen og infrastrukturen, opdateres relevant dokumentation således at denne altid er ajourført.

Der er defineret acceptabel brug af systemer for medarbejderne, hvilket bl.a. indebærer retningslinjer for at tilgå, bruge og eksportere data. Data anskues kategoriseret efter GDPR's kategorier hertil, og særlige procedurer gælder for visse datatyper.

Vi har procedurer som omhandler styring af bærbare medier, bortskaffelse af medier samt transport af bærbare, databærende medier, samt for klassifikation og mærkning af data. Dette betyder blandt andet (men er ikke afgrænset til) at data udelukkende må forefindes i systemer og på fysiske og virtuelle servere mærket og angivet til formålet. Kundedata må som udgangspunkt ikke forefindes andre steder, herunder lokalt, på USB-nøgler, på andre diske (flash drives) o. lign. En undtagelse herfor er hvis en kunde skriftligt har anmodet om at få udleveret data, eller hvis det er nødvendigt at flytte data mellem to servere, og transporten ikke kan ske via netværk.

Lagres data midlertidigt på sådanne USB-nøgler, drev o. lign., skal data i videst mulig udstrækning anonymiseres eller pseudonymiseres, og den fysiske enhed (herunder mapper på den) skal beskyttes af password. Disse medier må som udgangspunkt aldrig postforsendes til kunder, men skal transporteres af HeroBases medarbejdere, eller afhentes af kunden.

Når fysiske servere tages ud af drift, og data på harddiske ikke længere har behov for at forefindes på pgl. diske, skal diskene enten a) formateres således at genskabelse af data ikke længere er mulig, b) fysisk ødelægges og diskene bortskaffes af medarbejdere i HeroBases IT-afdeling, eller c) begge dele.

Adgangsstyring

Vi har en række procedurer som sikrer at adgangskontrol og rettighedstildeling sker i overensstemmelse med det fastlagte sikkerhedsniveau.

Kun medarbejdere, som har et arbejdsrelateret behov for at have adgang til systemer og data, får adgang til pågældende forretningssystemer med tilhørende data.

Afdelingslederne er ansvarlige for at adgangsrettigheder tildeles ud fra et arbejdsbetinget behov samt under hensyntagen til lovgivningsmæssige og kontraktlige forpligtigelser.

Vi har en række kontroller som kontrollerer at dette sker løbende, og at alle adgange modsvarer de arbejdsrelaterede behov i de enkelte funktioner og hos de enkelte medarbejdere.

Vi har defineret en række krav til alle enheders beskyttelse (PC'er, mobiltelefoner, tablets) samt passwords i alle forretningssystemer. Medarbejdere uddannes og kontrolleres løbende inden for disse områder.

Vi har en række procedurer som sikrer at kun en gruppe privilegeret personale har adgang til systemadministratorværktøjer, centrale servere (f.eks. domain controller), kildekode mv.

Produktionsservere og øvrige servere med produktionsdata og kundedata forefindes kun i HeroBases datacentre, og ikke på nogle kontorlokationer. Kun særligt betroede medarbejdere med et arbejdsrelateret behov har adgang til datacentrene. Disse adgange revalueres og efterses løbende.

Kryptografi

Vi har procedurer for anvendelse af kryptografi, herunder generering og håndtering af krypteringsnøgler og certifikater.

Dette betyder bl.a. at Hero Outbound skal have et gyldigt SSL-certifikat, HeroBase selv kontrollerer, således at dataudveksling kun sker sikkert og krypteret (gennem HTTPS). SSL-certifikater styres udelukkende af IT-

afdelingen, hvor applikationsarkitekten og netværksadministratoren har ansvaret for SSL-certifikater. Ingen certifikater må købes eller udstedes uden om disse.

Dette krav omfatter både adgang til Hero Outbound gennem brugergrænsefladen og gennem API.

Fysisk sikring og miljøsikring

Servere forefindes kun i datacentre udbudt af leverandører som har fået afgivet, og årligt kan fremvise, erklæringer på niveau med ISAE3402.

HeroBases kontorlokation er underlagt en række procedurer som sikrer kontoret samt materiale og enheder opbevaret på kontoret, upåagtet at servere kun forefindes i datacentre.

Dette betyder bl.a. procedurer rettet mod medarbejderne, der beskriver sikringstiltag for kontorer, fællesområder og lign. områder.

Driftssikkerhed

Driftsprocedurer og overvågning

Vi har driftsprocedurer for IT-afdelingens væsentligste arbejdsopgaver, og disse procedurer er omfattet af versionering og ændringsstyring.

Vi har defineret ansvar for at sikre, at der løbende bliver foretaget en vurdering af kapacitetsbehovet for kritiske it-systemer.

Pga. vores størrelse kan vi ikke have fuldstændigt overlap på samtlige funktioner, men jf. tidligere beskrivelse tilstræber vi qua funktionsadskillelse og grundig og løbende dokumentation og vidensdeling at undgå personafhængighed. IT-afdelingen, som ledes af HeroBases CTO, består primært af udviklere i en ”devops”-konstellation, hvor to mand er dedikeret til drift, optimering af servere og infrastruktur, overvågning og håndtering af operationelle issues, men hvor alle har drift som førsteprioritet i tilfælde af tekniske problemer på platformen eller informationssikkerhedsissues.

Alle instanser af Hero Outbound overvåges via monitoreringsværktøjer. Hermed overvåges blandt meget andet serveres fremkommelighed, CPU/memory/disk I&O forbrug, tilsvarende for databaseservere, lag (i millisekunder) mellem master- og slavedatabaser, tunge SQL queries foretaget af applikation eller direkte af en klient, o.m.a.

Der er for alle disse overvågningsområder defineret kritiske niveauer og værdier. Alarmer skal trigges når disse værdier nås, og sendes til nøglemedarbejdere på enten e-mail (for mindre kritiske opmærksomheder) og SMS (kritiske opmærksomheder).

Historiske logs og hændelser gennemgås løbende og struktureret med henblik på forbedringer og optimeringer.

Vi har procedurer for backups foruden løbende datareplikering, og backups brugbarhed til restore efterprøves løbende ved kontroller.

Udvikling af Hero Outbound, styring og kvalitetssikring

Udvikling af Hero Outbound, herunder release af ændringer, foregår efter HeroBases formaliserede og forankrede udviklingsmodel.

Udviklingsprocessen er HeroBases egen metode udledt af en agil tilgang til udvikling, SCRUM og RUP. Udvikling foregår i sprints men ikke af en eviggyldig specificeret varighed, idet sprints defineres ud fra prioriterede opgaver i backlog.

Med udgangspunkt i den klassiske projekttrekant bestående af tid, scope og ressourcer, er tid er den faktor, som definerer målsætningen for masterreleases, med en release mindst hver 4. uge, mens det tilstræbes at lave en masterrelease hver 3. uge. Kvalitet og færdigmeldte tests er dog altid at tilgodese over ønsket om at lave hyppigere releases, idet en nul-bug tolerance når ny kode deployes til produktion er altoverskyggende i forhold til ønske om at få nye funktioner/features hurtigt frigivet til kunderne.

Ved siden af masterreleases foretages hot fix releases med rettelse af decidere fejl og store uhensigtsmæssigheder. Væsentlige fejl og fundne sikkerhedssvagheder med prioritet 1 eller 2 (jf. HeroBases driftsprocedure) skal altid deployes hurtigst muligt og senest inden for 3 arbejdsdage.

Udvikling finder sted i udviklingsmiljøer, hvor kode branches ud fra hovedbranch/"default". Disse udviklingsbranches er forbundet til staging databasen, hvor testdata forefindes. Testdata og produktionsdata er således komplet adskilt, og kunders data må ikke kopieres fra master til staging uden godkendelse fra HeroBases CTO. Hvis denne tilladelse gives kan og vil det kun omfatte konfigurationsdata med henblik på at teste og udvikle op imod retvisende kompleks data for at sikre kvalitet af udvikling, men det må og kan aldrig omfatte data på kundens emner, medarbejdere eller andet som er personhenførbart og kategoriserbart i henhold til GDPR's artikler 6, 9 og 10.

Der funktionstestes i udviklingsbranches (også benævnt feature branches), hvorefter kode merges til præproduktion, videre til CX branch, videre til pre-release branch, videre til release branch hvorfra kode endegyldigt deployes til produktion.

Integrationstest med dertilhørende regressionstests og happy flow testing finder sted fra CX branch, prerelease branch og/eller release branch, hvor der testes på master databasen men på egne testdata. Kunders personhenførbare data indgår således ikke i tests og tilgås eller ses ikke af HeroBases medarbejdere i nogle af disse testfaser. Data i master databasen på egne konti er produceret så det strukturelt ligner produktionsdata, kunder arbejder med, hvormed datasikkerhed, fortrolighedsbehandling og samtidig kvalitetssikring sikres og balanceres.

Nedenfor ses i detaljer og kronologisk hvorledes alle cases behandles fra oprettelse, prioritering og godkendelse op gennem HeroBases udviklingsflow.

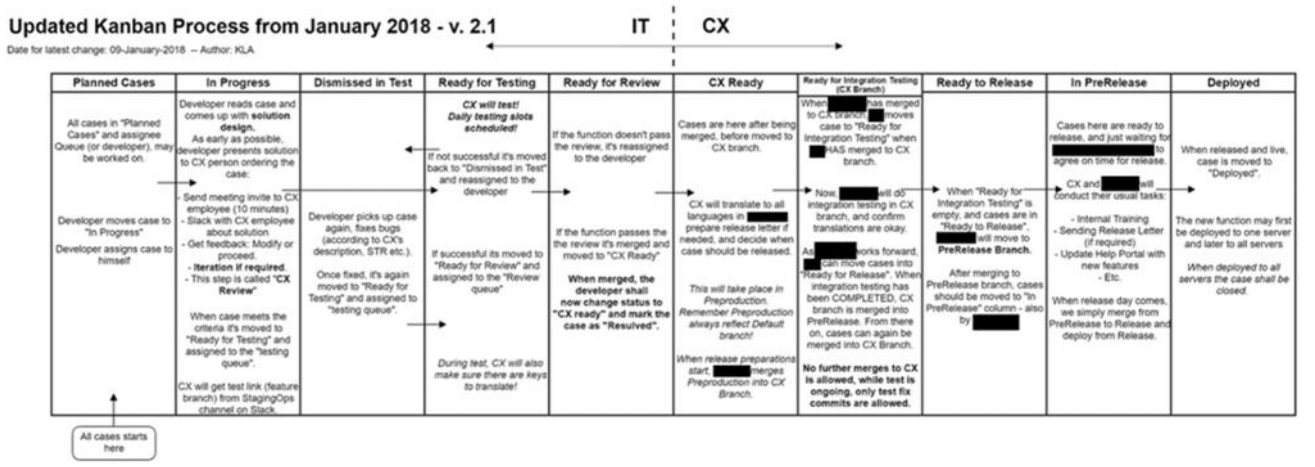

Fig. 2: Proces- og udviklingsmodel for Hero Outbound

HeroBases releasemanager er den dagligt ansvarlige for processen, og processen evalueres fast hver anden uge på et møde mellem release manager og HeroBases CTO.

Logning

Vi har procedurer som omhandler omfanget, behandling, beskyttelse og kontrol af logning på forskellige systemtyper.

Alle logins og væsentlige brugerhandlinger i Hero Outbound overvåges og logges. Logningen af væsentlige brugerhandlinger omhandler bl.a. dataeksport, således at kundeadministratorer har overblik over hvilke brugere, der tilgår og eksporterer data.

Alle ændringer på data registreres.

Alle væsentlige ændringer i konfigurationer registreres.

Disse registreringer er også tilgængelige for kundeadministratorer gennem synlige logs i brugergrænsefladen.

Logningsniveauet omfatter også medarbejdere hos HeroBase, hvormed det kontrolleres at disse ikke tilgår kundedata uden der er et arbejdsrelateret behov for det. Dette kontrolleres og efterprøves detaljeret på stikprøvebasis.

Kommunikationssikkerhed

Vi har procedurer for netværksstyring og overvågning, herunder vedligeholdelse af netværk og netværksudstyr.

Trafik på alle forbindelser og interfaces overvåges i forhold til datavolumen over perioder. Der er opsat alarmer som udløses og sendes til teknisk personale i tilfælde af anormaliteter (trafik spikes, væsentlige delays mellem master databaser og slave databaser, o.m.a.). På teleforbindelser bliver bl.a. antal provider kanaler, antal serverkanaler (Freeswitch kanaler) og antal igangværende opkald overvåget, og max-værdier for perioder logges.

Dette sikrer løbende korrekt kapacitetsstyring samt gardering mod misbrug.

Vi har desuden samarbejde med fraud-detekteringsafdelinger hos alle teleoperatører, vi benytter som underleverandører, som et ekstra lag af sikkerhed i forhold til misbrug.

Informationsudveksling sker kun via sikre forbindelser. Går dette via det offentlige internet bliver data krypteret (som udgangspunkt via HTTPS). Systemer som har mulighed for at kommunikere på interne forbindelser (på intern IP-adresse bag firewall - og mellem datacentre ad fiberforbindelse hvorigennem servere på forskellige lokationer også kan nå hinanden på intern IP-adresse) benytter denne metode til dataudveksling via LAN.

Anskaffelse, udvikling og vedligeholdelse af systemer

Vi har procedurer som sikrer en sikker styring af ændringer i forretningsunderstøttende systemer. Procedurerne foreskriver bl.a. at ændringslogs indhentes og evalueres, og at ændringer testes inden de frigives.

Idet alle væsentlige interne arbejdsprocesser er dokumenteret, bliver procesdokumentationen opdateret hvor nødvendigt, i forbindelse med ændringer.

Bemærk at dette afsnit og de procedurer, der henvises til, omhandler vedligeholdelse af og ændringer i forretningsunderstøttende systemer, ikke selve løsningen Hero Outbound. Procedurer og principper for ændringer i Hero Outbound er beskrevet i særskilt afsnit tidligere.

Leverandørforhold

Vi har i alle samarbejdsaftaler med leverandører defineret sikkerhedskrav og minimumskrav til ydelserne, vi modtager fra leverandøren.

Vi har sikret at de forhold, vi baserer vores aftale om brug af produktet og ydelsen Hero Outbound på over for vores kunder, er overensstemmende med de krav vi stiller til vores leverandører.

Vi gennemgår løbende og mindst årligt samarbejdsaftalerne, ligesom vi indhenter revisionserklæringer for de indgåede aftaler.

Vi har defineret ansvar for kvartalsvist at gennemgå rapporter fra de eksterne serviceleverandører på operationelt udstyr, omhandlende hændelser, problemer, fejl, nedbrud og logning.

Styring af informationssikkerhedsbrud og -hændelser

Informationssikkerhedsudvalget har defineret procedurer for informationssikkerhedsbrud og -hændelser, som er forankret i HeroBase og som ledelsen har ansvaret for overholdelsen af.

Vi definerer informationssikkerhedsbrud som:

- Detektering af succesfuld udefrakommende og uønsket indtrængen i systemer
- Fund af kundedata (hostet i masterdatabase for Hero Outbound) online, hvor der er åbenlys eller kraftig mistænke om at offentliggørelse af data ikke er sket med kundens godkendelse og forsæt
- Fund af data på nuværende eller tidligere medarbejdere i HeroBase online, hvor offentliggørelse af data er sket uden HeroBases medvirkende eller forsæt
- Fund af andre fortrolige forretningsdata online (efter samme forskrifter) defineret som kundekontrakter, omsætning eller informationer som er klassificeret som hemmelige efter nærmere definition af informationssikkerhedsudvalget

Vi definerer informationssikkerhedshændelser som:

- Hændelser som, hvis de ikke var blevet opdaget, kunne have ført til sikkerhedsbrud
- Situationer hvor utilsigtet data eller information ved et uheld (ved menneskelig fejl) er blevet sendt til andre modtagere end de tilsigtede, og det vurderes at dette kan medføre skade eller alvorlige konsekvenser for HeroBase

Der er defineret procedurer for begge, som beskriver for medarbejdere og ledere, hvordan de skal forholde sig ved brud og hændelser, inkl. (men ikke afgrænset til) indsamling af bevismateriale og kontakt til myndigheder, hvis nødvendigt.

Alle medarbejdere er bekendte med instrukserne og trænet heri.

Informationssikkerhedsaspekter ved nød-, beredskabs- og reetableringsstyring

Vi har defineret ansvar for udarbejdelse af nødplaner, beredskabsplaner og reetableringsplaner.

Vi har etableret tilstrækkelig redundans for at imødegå kravene til tilgængelighed og de garantier for oppetid, vi har kontrakt med vores kunder på.

Alle tekniske medarbejdere er trænet i planerne.

Planer og procedurer evalueres løbende og efter hvert operationelt issue, hvor menneskelig handling har været nødvendigt for at reetablere drift på dele af platformen.

Overensstemmelse

Vi kontrollerer løbende at regler og procedurer bliver efterlevet, fulgt og dokumenteret.

Vi sikrer at vi handler inden for gældende lovgivning og i øvrigt efterlever krav som stilles til dokumentation af national lovgivning.

Vi sikrer at persondata beskyttes og behandles i overensstemmelse med Persondataloven og GDPR.

ISO27001 har i årevis været brugt som referenceramme for informationssikkerhed i HeroBase og omkring udvikling og drift af Hero Outbound. Dette er vores første ISAE3402-erklæring på leverance af produktet og ydelsen Hero Outbound, hvorfor der er tale om en type I-erklæring. Det er forankret i ledelsen at efterlevelsen af regler og procedurer i vores informationssikkerhedsregelsæt, herunder kontroller som knytter sig til regler og procedurer, skal formaliseres, dokumenteres og underlægges årlig revision af en ekstern IT-revisor, hvorfor vi også for fremtiden vil få udarbejdet ISAE3402 (type II) erklæringer.

Komplementerende kontroller

HeroBase er over for vores kunder ansvarlige for at levere de ydelser og den drift, som er beskrevet i kontrakten omhandlende Hero Outbound mellem kunden og HeroBase.

Forhold, som ikke er omfattet af kontrakten, er kundens eget ansvar.

Oprettelse af brugere, beskyttelse af brugerinformationer og sikre login-procedurer er kundens ansvar. Kunden kan ved skriftlig henvendelse til HeroBase anmode om at få etableret ip-lås på kundens Hero Outbound-konto, hvormed login kun vil være muligt fra eksplicit definerede whitelistede ip-adresser. HeroBase anbefaler vores kunder at gøre dette i den udstrækning, det er muligt for kunden, for at beskytte kundens data og aktiviteter i Hero Outbound.

For så vidt angår data uploadet til Hero Outbound af kunden, er det en væsentlig ansvarsdeling at kunden er dataansvarlig og HeroBase er databehandler. HeroBase handler således alene ud fra instruks fra kunden. Kunden giver i kontrakten eller i databehandleraftalen HeroBase tilkendegivelse af, hvilke typer/kategorier af data, kunden har intentioner om at uploade til og behandle i Hero Outbound. Der skal forefindes en databehandleraftale mellem HeroBase og kunden.

For så vidt angår GDPR stiller HeroBase en række funktioner til rådighed på platformen Hero Outbound, som gør det muligt for kunden at leve op til GDPR's krav til dataansvarlige. Disse funktioner indbefatter (men er ikke afgrænset til) mulighed for at fremsøge data samt log over alle interaktioner mellem agent og "emner", mulighed for at berigtige data, mulighed for at slette data o.m.a.

Det er kundens ansvar at have defineret og forankret en procedure hos kunden, som sikrer efterlevelse af GDPR ved bl.a. at leve op til kravene om svartider ved henvendelser fra privatpersoner/datasubjekter. HeroBase stiller funktioner til rådighed gennem værktøjet Hero Outbound, men kan ikke holdes ansvarlig for kundens definition, forankring og efterlevelse af procedurer som skal sikre kundens overholdelse.

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

Til ledelsen hos HeroBase A/S, HeroBase A/S' kunder og deres revisorer.

Omfang

Vi har fået til opgave at afgive erklæring om HeroBase A/S' beskrivelse, som er gengivet i afsnit 2. Beskrivelsen, som i afsnit 1 er bekræftet af HeroBase A/S' ledelse, dækker virksomhedens behandling af kunders transaktioner i virksomhedens softwareløsning Hero Outbound pr. 1. september 2018 samt udformningen af de 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.

Vores konklusion udtrykkes med høj grad af sikkerhed.

HeroBase A/S' ansvar

HeroBase A/S er ansvarlig for udarbejdelsen af beskrivelsen (afsnit 2) og tilhørende udtalelse (afsnit 1), herunder fuldstændigheden, nøjagtigheden og måden, hvorpå beskrivelsen og udtalelse er præsenteret. HeroBase A/S er herudover ansvarlig for leveringen af de ydelser, beskrivelsen omfatter, for at anføre kontrolmål, og for udformningen, implementeringen og effektiviteten af kontrollerne for at nå de anførte kontrolmål.

REVI-IT A/S' uafhængighed og kvalitetsstyring

Vi har overholdt kravene til uafhængighed og andre etiske krav i IESBA's Etiske regler, som er baseret på grundlæggende principper om integritet, objektivitet, faglige kompetencer og fornøden omhu, fortrolighed samt professionel adfærd.

Firmaet anvender ISQC 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.

REVI-IT A/S' ansvar

Vores ansvar er på grundlag af vores handlinger at udtrykke en konklusion om HeroBase A/S' beskrivelse (afsnit 2) og om udformningen af de 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. 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.

Opgaven med afgivelse af en erklæring med sikkerhed om beskrivelsen og udformningen af kontroller hos en serviceleverandør omfatter udførelse af handlinger for at opnå bevis for oplysningerne i serviceleverandørens beskrivelse af sit system samt 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 udformede. En erklæringsopgave med sikkerhed af denne type omfatter endvidere 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 i afsnit 2.

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

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

HeroBase A/S' beskrivelse i afsnit 2 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 systemet, som hver enkelt kunde måtte anse for vigtige efter sine 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. Kriterierne, vi har anvendt ved udformningen af konklusionen, er de kriterier, der er beskrevet i HeroBase A/S' beskrivelse i afsnit 2, og det er på den baggrund vores vurdering,

(a) at beskrivelsen, således som det var udformet og implementeret per 1. september 2018, i alle væsentlige henseender er retvisende

(b) at kontrollerne, som knytter sig til de kontrolmål, der er anført i beskrivelsen, i alle væsentlige henseender var hensigtsmæssigt udformede per 1. september 2018.

Tiltænkte brugere og formål

Denne erklæring er udelukkende tiltænkt kunder, der har anvendt HeroBase A/S' udvikling og drift af softwaren Hero Outbound, og deres revisorer, som har en tilstrækkelig kompetence til at vurdere den medfølgende beskrivelse sammen med anden information, herunder information om kunders egne kontroller. Denne information tjener til opnåelse af en forståelse af kundernes informationssystemer, som er relevante for regnskabsaflæggelsen.

København, 1. september 2018

REVI-IT A/S
Statsautoriseret revisionsaktieselskab

Henrik Paaske
Statsautoriseret revisor

Martin Brogaard Nielsen
It-revisor, CISA, CIPP/E, CRISC, adm. direktør