Sikkerhedspolitik

Nærværende dokument beskriver de sikkerhedsforanstaltninger, som leverandøren har opstillet til den interne fysiske sikkerhed, datasikkerhed, logisk sikkerhed og sikkerhed i forbindelse med netværk, firewall og backup. Sikkerhedspolitikken er udarbejdet, så den overholder leverandørens erklæringer og godkendes årligt af det tilknyttede revisionsfirma jf. ISAE 3402 standarden.

Version 4.0506 – d. 6. maj 2014

vmware PARTNER PREMIER SERVICE PROVIDER
vmware vCLOUD POWERED
EY ISAE 3402 Type 2 Revisorerklæring
CITRIX PARTNER
CERTIFICERET IT-HOSTING
AAA Højeste kreditværdighed

1 FORMÅL

Formålet med nærværende dokument er, at beskrive de sikkerhedsforanstaltninger som Leverandøren har opstillet for at imødekomme egne krav til fysisk sikkerhed, datasikkerhed, logisk sikkerhed og sikkerhed i forbindelse med netværk, firewall og backup.

2 FYSISK SIKKERHED

Leverandørens datacenter er konstrueret af moderne udstyr, der sikrer et stabilt og fysisk sikkert driftsmiljø med et højt serviceniveau. Udstyret i datacenteret bliver løbende kontrolleret og opgraderet for at sikre den stabile drift.

Køling

Kølesystemets enheder er redundante, således at en vilkårlig komponent kan gå i stykker, uden at det får væsentlig betydning for temperaturen i driftscenteret.

Datacenteret er reguleret til en nedkølet lufts temperatur 23°C +/- 2°C, og en minimal luftfugtighed.

Brandsikring

Datacenteret er beskyttet mod brand via et "sniffer" system, som sikrer hurtig alarmering og aktivering af et Inergen-anlæg, så en eventuel lokal brand i en server ikke kan gøre skade på andet udstyr i datacenteret.

Oversvømmelse

Datacenteret ligger 70 meter over havoverfladen i et område der gennemsnitligt ligger 60 meter over havoverfladen. Datacenteret er beskyttet mod oversvømmelse, da alle servere står på et hævet EDB gulv ½ meter over jorden. I det underliggende gulvniveau er der afsat afløb med højvandslukke, som yderligere sikrer datacenteret mod vandskader.

Strøm og nødstrøm

Datacentret er forbundet med 2 separate strømtilslutninger, hvilket skaber redundans i tilfælde af strømsvigt. En lokal generatorstation leverer strøm til den daglige drift, mens en 500 kVA dieselgenerator tager over, i tilfælde af strømsvigt fra el-nettet. Dieselgeneratoren kan levere minimum 12 timers drift på én tank – hvis nødvendigt vil den løbende blive fyldt op af en tankvogn.

3 ADGANGSKONTROL

Det er udelukkende driftsteknikere, der har adgang til datacenteret. Alle besøg bliver desuden registreret og videooovervåget, og adgang kræver at der anvendes et unikt adgangskort. Hvis eksterne personer, såsom kunder, skal have adgang til datacenteret, kan det kun ske ved fremvisning af gyldigt ID og ifølge med en driftstekniker.

4 HARDWARE OG RESERVEDELE

Datacenteret holdes løbende opdateret med det nyeste og hurtigste hardware. Dette sker i tæt samarbejde med Dell og Cisco, som leverer alt datacenterets server- og netværksudstyr, med undtagelse af Fortigate Next Generation firewalls.

Der benyttes for så vidt muligt altid de samme leverandører af hardware til datacenteret. Dette gør det muligt at opbevare reservedele af alt hardware, så der hurtigt kan udskiftes de nødvendige dele i de forskellige servermodeller, hvis det bliver nødvendigt. Der vil altid være mindst en ekstra reservedel på adressen, så der meget hurtigt kan reageres på uheld og eventuel udskiftning af den defekte del.

5 BACKUP OG BRUGTE LAGERMEDIER

Leverandøren har et udvalg af backup muligheder. Genetablering af tabt data, kan efter anmodning fra kunder, under normale omstændigheder, ske inden for to timer. En primær backup bliver placeret i datacenteret, mens en sekundær backup er placeret på en sekundær lokation.

Harddiske og lagermedier der udgår fra driften, bliver destrueret på en måde, så det ikke er muligt at genetablere de ødelagte data igen. Alle genbrugte diske bliver formateret i overensstemmelse med gældende branchestandarder.

6 ANTIVIRUS

Alle arbejdsmaskiner og servere er udstyret med firewalls og antivirus software, der har til hensigt at blokere alle former for vira mv. Leverandørens netværksinfrastruktur er optimeret til, at kunne modstå alle former for hackerangreb, heriblandt DoS- og DDoS angreb, på en sådan måde, at kundernes løsninger forbliver upåvirket.

7 ADGANGSKODER

Leverandørens sikkerhedsprocedurer, dikterer at alle adgangskoder skal være komplekse og skiftes inden for rimelig tid – afhængig af produktet. Der gives desuden kun adgang til de systemer der er relevante for den enkelte medarbejder.

8 OVERVÅGNING

Datacenteret bliver overvåget på 3 niveauer;

Et fysisk niveau som overvåger datacenterets temperatur, brand, strømtilslutning og indbrud mv.

Et hardware niveau som måler på servernes strømtilslutning, kølere, temperatur, harddiske, controllere og ressourceforbrug.

Et serviceniveau som måler på de forskellige tjenester og applikationer.

Uanset hvor problemet opstår, bliver en vagthavende alarmeret og informeret, så han kan tage de rette forholdsregler.

9 VAGTPROCEDURER

Der er telefonisk support inden for Leverandørens normale åbningstid.

Uden for normal åbningstid bemandes Leverandørens vagttelefon 24/7, 365 dage om året. Vagttelefonen bemandes af en 1. level supporter, der kan eskalere til en 2. level supporter, der ligeledes er på vagt 24/7, 365 dage om året.

Reaktionstiden for vagten og påbegyndt fejlfinding afhænger af kundens SLA niveau. Systemfejl vurderes og prioriteres ligeledes efter SLA niveau.

10 SERVICEVINDUE OG DRIFTSUDMELDINGER

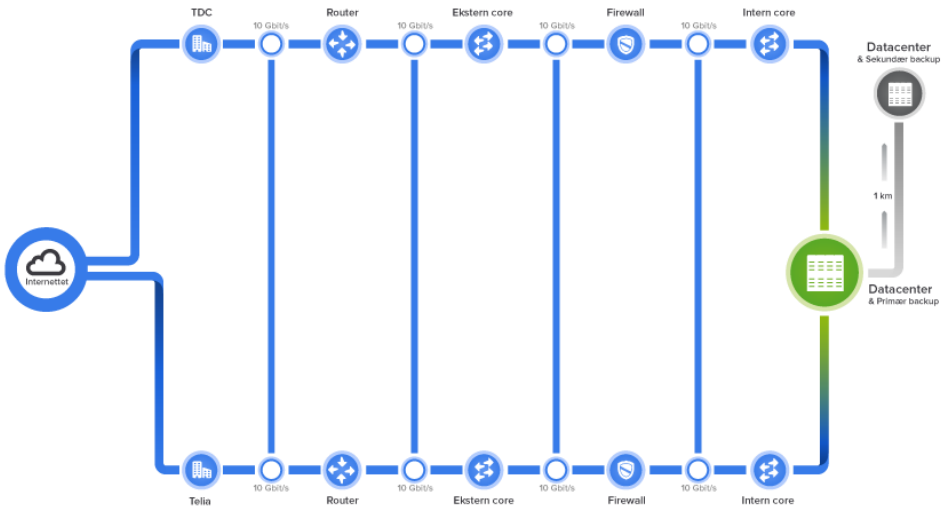
Alle opdateringer, systemarbejde og vedligehold bliver som udgangspunkt udført i tidsrummet 00:00 – 05:00 på alle ugens dage.

I tilfælde, hvor kunder med egne servere eller vitale dele af driften er påvirket, bliver der udsendt e-mails til de berørte kunder. Hvis nedetiden overstiger 15 minutter, bliver dette desuden udmeldt på driftssiden, der løbende bliver opdateret med relevant information.

11 NETVÆRK

Leverandørens netværk er redundant, både med henblik på internetforbindelser, backbone netværk og infrastruktur. Leverandøren har 2 x 10Gbit fiber-forbindelser til henholdsvis TDC og Telia, som befinder sig på hvert deres netværk.

Netværksdiagram:



12 TEKNISK DOKUMENTATION

Drift dokumenteres efter gældende interne standarter. Visse systemer kræver godkendelse af eksterne revisorer i forbindelse med ISO og PCI certificeringer af betalingsgateway og lign.

Der foreligger teknisk dokumentation på alle kritiske systemer som Leverandøren har i drift. Dokumentation samles ligeledes i en fælles videns base for interne systemfolk.

13 FASTE PROCEDURER VED KATASTROFENEDBRUD

Der forefindes procedurer for alle kritiske driftsoperationer og nødprocedurer for katastrofenedbrud. I visse tilfælde består procedurerne af tilkaldelse af eksterne eksperter, eksempelvis inden for køl, el og brandslukning.