Sikkerhedspolitik

Denne sikkerhedspolitik beskriver de krav som Leverandøren stiller til den interne fysiske sikkerhed, datasikkerhed, logiske sikkerhed og sikkerhed i forbindelse med netværk og firewalls. Sikkerhedspolitikken definerer det grundlæggende niveau for Leverandørens infrastruktur og omhandler ikke forhold vedrørende specifikke kunder, services eller produkter.

Sikkerhedspolitikken er udarbejdet så den overholder Leverandørens ISO certificering (Dansk Standard), PCI Certificering (Fort Consult) og godkendes årligt af det tilknyttede revisionsfirma jævnfør ISAE 3402 standarden. Slutteligt er forholdene i centeret etableret for at imødekomme ønsker fra kunder, forhandlere og partnere.

Version 3.1003 – d. 3. oktober 2013

vmware PARTNER PREMIER SERVICE PROVIDER
vmware vCLOUD POWERED
BFiH CERTIFICERET IT-HOSTING
CITRIX PARTNER
Deloitte. ISAE 3402
AAA

INDHOLDSFORTEGNELSE

1. Introduktion 3
1.1. Formål 3
2. Fysisk sikkerhed 3
2.1. Miljø og sikring 3
2.2. Adgangskontrol 4
3. Hardware 4
3.1. Redundansniveau 4
3.2. Reservedele og udskiftning 4
4. Datasikkerhed 5
4.1. Brugte lagermedier 5
4.2. Sikkerhedskopiering (Backup) 5
4.3. Antivirus 5
5. Logisk sikkerhed 5
5.1. Adgangskoder 5
5.2. Overvågning og rapportering 5
5.3. Vagtprocedurer 6
5.4. Driftsudmeldinger 6
6. Netværk 7
6.1. Netværksdiagram 7
7. Dokumentation 7
7.1. Teknisk dokumentation 7
7.2. Procedurer 7

1. INTRODUKTION

1.1. FORMÅL

Leverandørens sikkerhedspolitik med krav til sikkerhed og procedurer har følgende formål:

1.1.1. Datacenteret skal være et stabilt og fysisk sikker driftsmiljø med højt serviceniveau.

1.1.2. Leverandørens medarbejdere har kun adgang til den nødvendige mængde data, der relatere sig til personens arbejdsområder.

1.1.3. Uvedkommende personer kan ikke få adgang til datacenterets servere eller andre maskiner tilknyttet serverne, hvorpå der forefindes følsomme informationer.

1.1.4. Systemer, servere og services skal holdes tilgængelige 24/7/365, i så vid mulig udstrækning, selvom datacenteret udsættes for strømsvigt, brand, overgravede kabler eller lign. force majeure situationer.

2. FYSISK SIKKERHED

2.1. MILJØ OG SIKRING

Datacenteret er beskyttet med udstyr der kendetegner et professionelt hostingmiljø. Udstyr og procedurer i centeret bliver løbende evalueret af både intern og ekstern ekspertise.

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

Der leveres en nedkølet luft med temperaturen 23°C +/- 2°C, og en minimal luftfugtighed.

2.1.2. **Brandsikring**
Brandsikringen beskytter datacenteret via et "sniffer" system, som sikrer hurtig alarmering og aktivering af inergenanlæg, så en eventuel lokal brand i en server, ikke kan gøre skade på andet udstyr i centeret.

2.1.3. **Oversvømmelse**
Datacenteret ligger 70 meter over havoverfladen i et område der gennemsnitligt ligger omkring 60 meter over. Datacenteret er beskyttet mod vand, idet alle servere står på et hævet gulv, 0,5 m. over niveau. I det underliggende niveau er der afsat afløb med højvandslukke.

2.1.4. Strøm og nødstrøm

Alle strøminstallationer i datacenteret er forsynet fra UPS. Ved strømsvigt fra el-nettet kan dieselgenerator levere minimum 10 timers drift på én tank. Ved strømsvigt af længere varighed, bliver generatoren forsynet med yderligere diesel fra en tankvogn.

Strøminstallationerne betragtes som redundante fordi hovedforsyningskablet, UPS og dieselgenerator er hinandens redundante komponenter.

2.2. ADGANGSKONTROL

Det er udelukkende clearede driftsteknikere der har adgang til datacenteret. Ved adgang til centeret sker der logning ud fra adgangskort og video overvågning.

2.2.1. Adgang for eksterne personer

Der er kun adgang til datacenteret ved aflevering af gyldigt ID. Adgang til selve serverrummet sker kun ifølge med én af Leverandørens medarbejdere.

2.2.2. Indbrud, videoovervågning og sabotage

Datacenteret har sikret gulve og mure uden vinduer. Alle forskrifter i forbindelse med personsikkerhed er iagttaget. Der er tilknyttede vagtordning 24 timer i døgnet, året rundt. Datacenteret er ude og inde forsynet med kameraer, IR sensorer og området er indhegnet.

3. HARDWARE

3.1. REDUNDANSNIVEAU

For at sikre den bedste SLA til kritiske applikationer, konfigureres redundante miljøer hertil. Kravene udspecificeres til den enkelte opgave, men er altid underbygget af de redundante teknologier der ligger i hostingcenterets Cisco/HP baserede netværk. Her ud over underbygges redundante setups oftest af SAN, Blades og/eller virtualisering.

3.2. RESERVEDELE OG UDSKIFTNING

Der benyttes så vidt mulig benyttes samme leverandør af hardware til hostingcenteret. Dette giver mulighed for opbevaring af reserve hardware til udskiftning i alle server-modeller. Der opbevares altid mindst en ekstra enhed (server, switch og lign.) på adressen, for hurtig udskiftning af defekte dele. Såfremt specielle modeller/teknologier anvendes, tilkøbes ekstra *onsite support*, så dele kan udskiftes inden for 4/24/48 timer efter behov.

4. DATASIKKERHED

4.1. BRUGTE LAGERMEDIER

Lagermedier der udgår fra driften destrueres, så det på ingen måde er muligt at genetablere dataene igen. Diske der genbruges i servere bliver før genbrug, formateret i overensstemmelse med følgende standarder; US Department of Defense 5220.22 M, German VISTR, Russian GOST p50739-95, Gutmann method.

4.2. SIKKERHEDSKOPIERING (BACKUP)

Primære backupenheder er placeret i datacenteret og håndterer alle typer af data (databaser, Exchange, o.l.). Backup procedurer kører dagligt, med minimum 14 dages historik. Genetablering af backup skal kunne ske på anmodning fra kunder og skal under normale omstændigheder kunne gøres inden for to timer.

4.3. ANTIVIRUS

Alle Leverandørens interne management systemer (arbejdsstationer) overvåges af antivirus.

5. LOGISK SIKKERHED

5.1. ADGANGSKODER

For interne systemer gælder at adgangskoder skal være komplekse og skiftes inden for rimelig tid, bestemt ud fra produktet.

Der gives kun adgang til de systemer der er relevante for medarbejderen. System passwords opbevares krypteret, hvor kun udvalgte medarbejdere har adgang.

5.2. OVERVÅGNING OG RAPPORTERING

Der overvåges på 3 niveauer i datacenteret;

Fysisk: Datacenter temperatur, brand, strøm, indbrud osv.

Udstyr: Strøm, fans, temperatur, diske, controllere, on/off osv.

Service: Tjenester på server/udstyr f.eks. smtp på mail servere, http på web, interface på netværk osv.

Alle alarmer eskaleres efter interne procedurer igennem mail og SMS til vagthavende.

5.3. VAGTPROCEDURER

5.3.1. 24 / 7 og 8-16

Der er telefonisk support mandag til torsdag 08:00 til 16:00 og fredag 08:00 – 15:00, defineret som normal åbningstid.

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

5.3.2. Reaktionstid for vagt

For kritiske systemer er reaktionstiden for vagten døgnet rundt 10 minutter, og påbegyndt fejlfinding er inden for 30 min. Ikke kritiske systemer vurderes og prioriteres efter tildelt intern SLA.

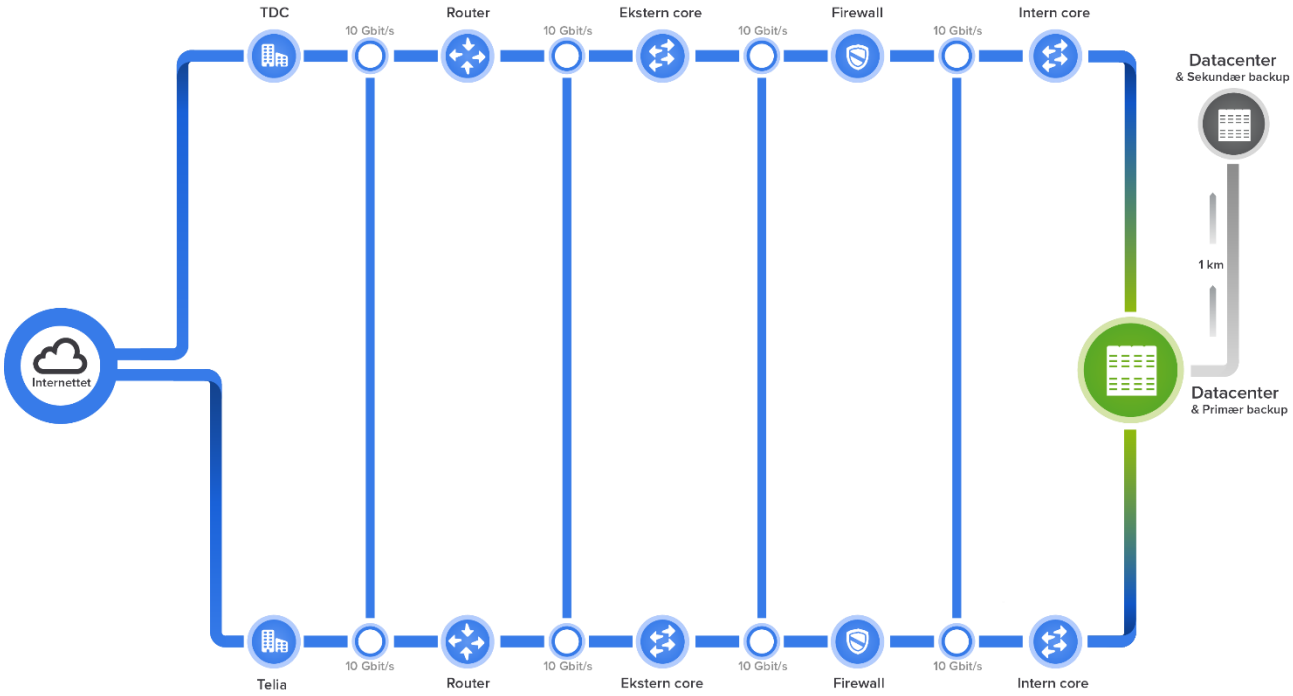
5.4. DRIFTSUDMELDINGER

Planlagt systemarbejde udføres så vidt muligt om natten, med start ved midnat kl. 00.00. Systemarbejdet annonceres som minimum på vores driftsside. I særlige tilfælde, hvor dedikerede server kunder eller vitale dele af driften er påvirket, udsendes der e-mail til relevante kunder.

I tilfælde af nedbrud af varighed over 15 min., beskrives problemet på vores driftsside. Driftssiden holdes løbende opdateret med relevant information. I særlig alvorlige tilfælde udsendes e-mail til relevante kunder. Listen med drift-status opdateres live.

6. NETVÆRK

6.1. NETVÆRKSDIAGRAM



Netværksdiagrammer over hele datacenteret og det interne netværk bliver løbende gennemgået og opdateret, såfremt der er sket ændringer i netværket.

7. DOKUMENTATION

7.1. 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 i drift. Dokumentation samles ligeså i en fælles knowledgebase for interne systemfolk.

7.2. PROCEDURER

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