4dimensions

Informationssikkerhedsikkerhedspolitik

Version: 1.09

Dokument startet: 2019

4dimensions

INDHOLDSFORTEGNELSE

1. INTRODUKTION

Denne sikkerhedspolitik beskriver de krav 4 dimensions A/S stiller til den interne fysiske sikkerhed, datasikkerhed, logiske sikkerhed og sikkerhed i forbindelse med netværk og firewalls. Sikkerhedspolitikken definerer det grundlæggende niveau for 4 dimensions A/Ss infrastruktur og omhandler ikke forhold vedrørende specifikke kunder, services eller produkter.

Sikkerhedspolitikken er udarbejdet så den overholder 4 dimensions A/S interne retningslinjer og procedure. Slutteligt er forholdene i centeret etableret for at imødekomme ønsker fra kunder, forhandlere og partnere.

1.1. FORMÅL

4 dimensions A/Ss sikkerhedspolitik med krav til sikkerhed og procedurer har følgende formål:

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

4 dimensions A/Ss medarbejdere har kun adgang til den nødvendige mængde data, der relatere sig til personens arbejdsområder.

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

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.

1.2. Omfang

Informationssikkerhedspolitikken er det dokument, der angiver de beslutninger, som ledelsen i 4dimensions, har truffet med henblik på nærmere at fastlægge det tilstrækkelige sikkerhedsniveau samt definere de krav, der stilles for at sikkerhedsniveauet opretholdes. Derfor fastlægges omfanget af sikkerhedsinformationspolitikken således:

- Informationssikkerhedspolitikken gælder for alle ansatte i 4dimensions uanset ansættelses.
- Informationspolitikken gælder for alle, systemer og alle data i 4dimensions besidelse.

- Leverandører og samarbejdspartnere, som har fysisk eller logisk adgang til organisationens systemer og data, skal ligeledes have kenskab til og følge Informationssikkerhedspolitikken.
- Informationssikkerhedspolitikken udgør 4dimensions informationssikkerhedsstartegi.
- Informationssikkerhedspolitikken dækker alle tekniske og administrative forhold, der har direkte eller indirekte indflydelse på drift og brug af 4dimensions it-systemer.
- Informationssikkerhedspolitikken godkendes af direktionen og revideres en gang årligt for at sikre at den er i overensstemmelse med de sikkerhedsmålsætninger, som 4dimensions arbejder efter.

2. Risikovurdering

Det sikkerhedsniveau, denne sikkerhedspolitik er fastsat på baggrund af er, 4dimensions vurdering af de ricici, som vi ønsker at imødegå.

IT-vurderingen opdateres årligt og ved evt. større ændringer i IT-systemerne, ændringer i anvendelse af systemerne eller ved større organisatoriske ændringer med efterfølgende tilretninger af informationssikkerhedspolitikken, retningslinjer mm.

3. Organisering og ansvar

3.1. Interne organisatoriske forhold

Organisering af informationssikkerheden i 4dimensions er defineret i sikkerhedspolitikken. Bestyrelsen har det overordnede ansvar for at sikre at 4dimensions ledelse har defineret en informationssikkerhedspolitik.
Ledelsen beslutter overordnede strategiske projekter af informationssikkerhedsmæssige karakter, men har i praksis delegeret det daglige ansvar for informationssikkerheden til CTO'en. Ledelsen vil uddelegere ansvar og opgaver vedrørende de enkelte funktionsområder herunder også for vejledning og instruktion af medarbejdere.

3.2. Brugeradfærd

Opretholdelse af det ønskede sikkerhedsniveau, afhænger af at vi alle tager ansvar for informationssikkerheden. Alle ansatte skal være bekendt med informationssikkerheden. Alle ansatte skal være bekendt med sikkerhedspolitikken og gældende retningslinjer for ønsket adfærd.
Anvendelse af IT og behandling af data er selvfølgelige redskaber i varetagelse af daglige arbejdsopgaver. Håndtering af vores redskaber bør ske med omtanke og almindelig sund fornuft. Det er således tilstrækkeligt og vigtigt at følge disse få retningslinjer:

- Persondata behandles i alle tilfælde fortroligt.
- Der anvendes personligt login og password og password skiftes mindst hver 3. måned
- Datamedier med persondata og vigtige informationer behandles og beskyttes med omhu mod at uvedkommende får adgang til dem. Mobilt udstyr beskyttes og opbevares så andre ikke kan få adgang til det.
- Det er vigtigt at kunne anvende Internettet i mange sammenhænge. Besøg på sider med racistisk, uetisk, eller pornografisk indhold er ikke acceptabelt i forbindelse med de daglige arbejdsopgaver.

- Mail anvendes til kommunikation på mange niveauer – også til privat kommunikation, men bør holdes på et rimeligt niveau. Privat kommunikation skal tydeligt markeres.
- Hvis man oplever at der sker brud på informationssikkerheden skal hændelsen rapporteres til sin nærmeste leder og CTO

3.3. Ansættelsesforholdet

Alle medarbejdere har medansvar for at opretholde det ønskede sikkerhedsniveau i 4dimensions. For at kunne leve op til ansvaret, er det den enkelte afdelingsleders ansvar at sørge for instruktion i forhold til anvendelse af systemer i det daglige arbejde, samt i forhold til den ønskede adfærd for informationssikkerhed.
Alle medarbejdere skal:

- Have et generelt kendskab til informationssikkerhed.
- Kende deres ansvar for sikkerheden.
- Sikre deres personlige adgangskoder.
- Passe på organisationens IT-udstyr.
- Deltage aktivt i rettelse af fejl, løsning af problemer og forbedringer af sikkerheden.

3.4. Sikkerhedsprocedurer før ansættelse:

Der skal være procedurer, der sikrer ansættelse af kompetente og sikkerhedsmæssigt egnede medarbejdere. Medarbejdere, der skal arbejde med fortrolige oplysninger, kan pålægges at fremlægge straffeattest inden ansættelse.
Det skal sikres at der foreligger ansættelseskontrakter indeholdende tavshedserklæring på alle ansatte.

3.5. Ansættelses ophør:

Der er procedurer der sikrer at IT-aktiver returneres, og at adgange og rettigheder ophører ved ansættelsesforhgoldets ophør. Brugerkonti deaktiveres.

4. Mobilt udstyr og fjernarbejdspladser

Informationssikkerhedspolitikken gælder for alt it-udstyr tilhørende 4dimensions. I retningslinjen for medarbejdere fastlægges de regler, som skal overholdes ved brug af af mobilt udstyr og hjemmearbejdspladser.

5. Rapportering af sikkerhedshændelser:

En væsentlig del i informationssikkerhedsarbejdet består i at reagere på hændelser af sikkerhedsmæsssig karakter. Derfor skal sikkerhedsmæssige hændelser rapporteres, og der skal ske opfølgning herpå. Alle medarbejdere har pligt til at rapportere sikkerhedshændelser til nærmeste leder og CTO. Rapportering af sikkerhedshændelser er beskrevet i retningslinjer herfor. CTO og ledelsen orienteres om indtrufne hændelser.

6. FYSISK SIKKERHED

6.1. 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.

6.1.1. 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 22˚C +/- 2˚C, og en minimal luftfugtighed.

6.1.2. 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.

6.1.3. Oversvømmelse

Datacenteret ligger 25 meter over havoverfladen i et område der gennemsnitligt ligger omkring 20 meter over. Datacenteret er beskyttet mod vand, idet alle servere står på et hævet gulv, 1,5 m. over niveau. I det underliggende niveau er der afsat afløb med højvandslukke.

6.1.4. 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.

6.2. ADGANGSKONTROL

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

6.2.1. ADGANG FOR EKSTERNE PERSONER

Der er kun adgang til datacenteret ved aflevering af gyldigt ID. Adgang til selve server-rummet sker kun ifølge med én 4 dimensions A/S ansat.

6.2.2. 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.

7. HARDWARE

7.1. 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, FortiGate og Dell baserede netværk. Her ud over underbygges redundante setups oftest af SAN, Blades og/eller virtualisering.

7.2. SPAREPARTS OG UDSKIFTNING

Der benyttes så vidt mulig benyttes samme leverandør af hardware til hostingcenteret. Dette giver mulighed for opbevaring af spareparts til udskiftning i alle server-modeller. Der opbevares altid mindst en ekstra enhed (server, switch, etc) på adressen, for hurtig udskiftning af defekte dele.

Såfremt specielle modeller/teknologier anvendes, tilkøbes ekstra onsite support, så dele kan udskiftes inden for 4 timer efter behov.

8. DATASIKKERHED

8.1. 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.

8.2. 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 indenfor to timer.

Vores HCI infrastuktur kører backup hver time, og gemmer som standard time backup for de første 24 timer. Derefter vil der være daglige backup i minimum 30 dage.

Genetablering fra backup i HCI infrastruktur udføres normalt af en tekniker fra 4 dimensions A/S, og vil under normale omstændigheder være udført inden for 15 minutter.

8.3. ANTIVIRUS og kryptering af arbejdsstationer

Alle 4 dimensions A/Ss interne management systemer (arbejdsstationer og bærbare) overvåges af antivirus og kører fuld disk kryptering.

9. LOGISK SIKKERHED

9.1. ADGANGSKODER

For 4 dimensions A/S 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.

Der anvendes en enterprise passwords manager, som sikrer den enkelte medarbejder kun har adgang til de koder der er nødvendige for at løse opgaven. Softwaren fører desuden fuld log over hvem der tilgår hvilke koder og hvornår.

9.2. 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 VM'er/server/udstyr f.eks. smtp på mail servere, http på web, interface på netværk osv, tilgængelig diskplads, forbrug af RAM og CPU og meget mere.

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

9.3. VAGTPROCEDURER

9.3.1. 24/7 & 730-1630

Der er telefonisk support mandag til torsdag 07:30 til 16:30 og fredag 07:30 – 16:00, defineret som normal åbningstid.

Uden for normal åbningstid er der 24/7 vagttelefon 365 dage om året.

Vagttelefonen bemandes af 1. level supporter, der kan eskalere til 2. level der også er på 24/7 vagt.

9.3.2 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.

9.4. DRIFTSUDMELDINGER

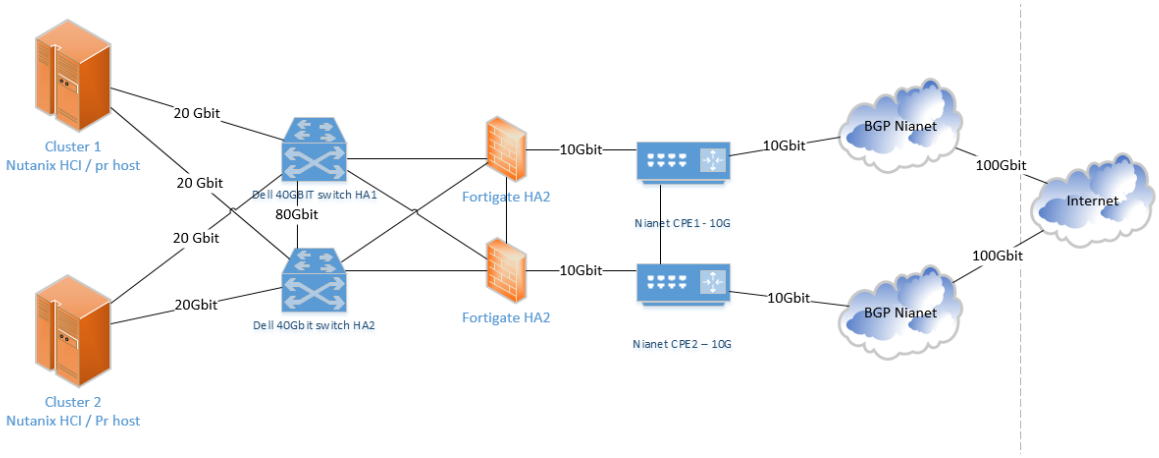
Planlagt systemarbejde udføres så vidt muligt om natten, med start ved midnat kl. 00.00. Systemarbejdet annonceres som minimum på vores driftsside. I særlige tilfælde, hvor dedikerede server kunder eller vitale dele af driften er påvirket, udsendes der e-mail til relevante kunder.

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.

10.NETVÆRK

10.1. NETVÆRKSDIAGRAM



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

11.DOKUMENTATION

11.1. TEKNISK DOKUMENTATION

Drift dokumenteres efter gældende interne standarter.

Der foreligger teknisk dokumentation på alle kritiske systemer i drift. Dokumentation samles ligeså i fælles knowledgebase for interne systemfolk.

11.2. 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.