STATENS IT

Bilag 11
Statens It's standarddriftsplatform

2014, version 2014-1

Indhold

1 Indledning

Den 1. januar 2010 fik Statens It ansvar for alle opgaver vedrørende administrativ it, it-infrastruktur samt en række opgaver vedrørende drift, vedligehold og brugeradministration af fag-it for en række ministerområder. Statens It er herigennem med til at skabe fundamentet for den videre digitalisering af staten.

Statens It har ansvaret for at drive en effektiv it-understøttelse og sikre en høj og ensartet it-service på tværs af staten. Hovedopgaverne omfatter drift, support, udvikling og harmonisering af it i staten.

I 2011 blev Statens It's datacenter implementeret og udgør i dag fundamentet for den standarddriftsplatform, som skal gøre det muligt for Statens It at levere sikker og stabil it-drift, der understøtter kundens forretning samt bidrager til at optimere it-ressourceforbruget i staten som helhed.

1.1 Formål

Formålet med dette dokument er at beskrive den standarddriftsplatform, som baseret på best practice, kendte standarder som ISO 27001 standarden samt solide teknologier, gør Statens It i stand til at levere den bedst mulige it-understøttelse til kundens forretning.

Dokumentet skal understøtte udviklingsprojekter for kundens fagapplikationer, som er beskrevet i aftalekompleksets bilag 6 – Snitflader mellem Kunden og Statens It, og derved give en hurtigere og mere smidig implementering i standarddriftsplatformen. Dette forudsætter dog, at der fra leverandørens side leves op til de beskrevne anbefalinger, der er formuleret på baggrund af arkitektur og sikkerhed i standarddriftsplatformen. Såfremt sikkerhedsanbefalingerne ikke følges, er det kundens fulde ansvar jf. ansvarsfordeling beskrevet i aftalekompleksets bilag 4 – Informationssikkerhed.

Bilag 11 er vejledende, og Statens It anbefaler de standarder, der er velafprøvede. Hvis anbefalingerne ikke følges, kan etablerings- og driftsomkostningerne stige og Statens It kan ikke garantere SLA på tilgængelighed og løsningstid. Der henvises til bilag 6, afsnit 8.1.

Såfremt det ikke er muligt at leve op til specifikationerne i dokumentet, skal der rettes henvendelse til Statens It med henblik på indgåelse af en særlig aftale.

Det påhviler i den forbindelse kunden til enhver tid at sikre compliance i forhold til bilag 11 med tilhørende underbilag.

2 Læsevejledning

Målgruppen for dette dokument er Statens It's kunder, herunder systemejere, samt tredjepartsleverandører.

Det forudsættes, at læseren er bekendt med de mest generelle begreber inden for it.

I afsnit 3 forklares referencearkitekturen for systemarkitektur og netværkssikkerhedszoner. Dette fungerer som rammen for løsninger, som skal implementeres i Statens It's standarddriftsplatform, herunder Statens It's datacenter.

I afsnit 4 beskrives de teknologier, som udgør Statens It's standarddriftsplatform. Det forventes, at nye løsninger baseres på og er i overensstemmelse med disse teknologier.

I afsnit 5 beskrives de services, som generelt stilles til rådighed for løsninger på Statens It's driftsplatform. Det forventes, at nye løsninger, i den udstrækning det er nødvendigt, anvender de tilgængelige services, herunder standarder.

Afsnit 6 omhandler rammerne for Statens It's teknologivalg.

2.1 Underbilag

Dette bilag er holdt fri af konfigurationsspecifikke detaljer, da disse vil være genstand jævnlig opdatering. Der er oprettet en række underbilag, som vil indeholde et mere specifikt detaljeringsniveau.

A) Referencemodeller for løsninger i Statens It's standarddriftsplatform
B) Standardserverkonfiguration i Statens It's standarddriftsplatform
C) Backuppolitik i Statens It's standarddriftsplatform
D) Teknologivalg

3 Referencearkitektur

3.1 Formål

Formålet med afsnittet er at beskrive Statens It's anbefalede systemarkitektur samt de netværkssikkerhedszoner, der anvendes i Statens It's datacenter. Sammenhængen mellem disse to begreber beskrives i afsnittet med referencemodeller, der viser anvendelsen af systemarkitektur i netværkssikkerhedszonerne. Statens it fokusere på it sikkerhed, samarbejder med GovCERT og følger deres anbefalinger samt markedes best practice.

3.1.1 Statens It's anbefaling til valg at arkitektur

Det er Statens It's anbefaling, at alle løsninger baserer sig på en arkitektur, der overholder referencemodel 1 for eksternt vendte og referencemodel 5 for internt vendte løsninger, dvs., at alle logiske lag i en løsning er separeret, både logisk og sikkerhedsmæssigt.

3.2 Systemarkitektur

For at imødekomme Statens It's arkitekturprincipper skal de løsninger, der implementeres gøre brug af fler-lags-arkitektur.

Princip	Beskrivelse
Standardisering	En øget standardisering giver mulighed for konsolidering af it-arkitekturen.
Genbrugelighed	Genbrug af eksisterende løsninger i stedet for ny udvikling eller nyanskaffelser
Skalerbarhed	En løsningsarkitektur skal kunne skaleres, således den er i stand til at understøtte en øget eller ændret behovssituation.
Sikkerhed	Sikkerhedsaspektet skal tænkes ind i alle løsninger

Ved at opbygge en løsning i flere lag vil der være øgede muligheder for udvikling og modificering af de enkelte lag, uden at hele løsningen skal omstruktureres.

3.2.1 Logiske arkitekturlag

Flerlags-arkitektur er en klient-server-arkitektur, hvor løsningens komponenter er separeret i logiske arkitekturlag: præsentations-, forretnings- og datalogik.

Figur 1 - Logiske arkitekturlag

3.2.1.1 Præsentationslogiklag

Øverste lag af en løsning består typisk af en klientapplikation og en eller flere servere til distribuering af præsentationslogikken. Klientapplikationen kan enten være egenudviklet eller browserbaseret og afvikles på en klient enhed. I dette dokument er præsentationslogikken udelukkende fokuseret omkring den serverbaserede del af præsentationslogikken.

3.2.1.2 Forretningslogiklag

Midterste lag af en løsning håndterer den forretningsmæssige processering af input fra præsentationslaget og data fra datalogiklaget.

I forretningslogiklaget håndteres forretningsregler samt forretningspolitikker, såsom autentificering og autorisation.

3.2.1.3 Datalogiklag

Nederste lag af en løsning håndterer lagring af data.

3.3 Netværkssikkerhedszoner

Netværkssikkerhedszoner er fundamentet i implementeringen af den net-værkssikkerhed, der danner rammen for Statens It's standarddriftsplatform.

En netværkssikkerhedszone er karakteriseret ved at være adskilt med en aktiv sikkerhedskomponent, og at det kun er tilladt for indhold i en sikkerhedszone at tilgå indhold i samme zone eller nabozoner.

Nedenstående tabel viser, hvilke sikkerhedsmæssige principper, Statens It anbefaler i forhold til netværkssikkerhedszoner og udvikling af løsninger.

Princip	Beskrivelse
Sikkerhed ved dybde	En løsning bør separeres i flere niveauer af sikkerhed, således at kompromitteringen af en enkelt komponent ikke eksponerer hele løsningen.
Afskærmning	Komponenter på samme sikkerhedsniveau bør adskilles logisk og isoleret ved brug af passende sikkerhedskomponenter. Dette sikrer, at løsninger på samme sikkerhedsniveau ikke kompromitterer hinanden.
Minimér angrebsflader	Antallet af tilgange til en løsning, på hvert sikkerhedsniveau, bør holdes til et minimum og adgangskontrolleres.

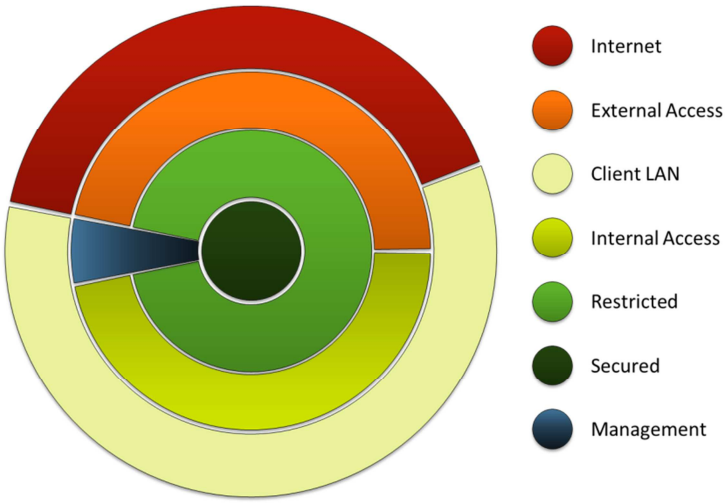
Princippet om ”Sikkerhed ved dybde” er implementeret i Statens It ved etablering af flere lag af netværkssikkerhedszoner adskilt af fysiske sikkerhedskomponenter i form af firewalls.

Princippet om ”Afskærmning” er implementeret i Statens It ved etablering af dels netværkssegmenteringer samt logisk ved stram styring af rettigheder.

Antallet af angrebsflader minimeres ved dels at holde indholdet i mindre sikre netværkssikkerhedszoner til et minimum samt stram kontrol med firewall åbninger og krav om protokol minimering i forhold til de etablerede løsninger jf. princippet ”Minimér angrebsflader”.

Netværkssikkerhedszonernes opbygning og anvendelse gennemgås i det følgende og sammenhængen til systemarkitekturen tydeliggøres i det efterfølgende afsnit.

Netværkssikkerhedszonerne i standarddriftsplatformen er illustreret i figur 2 nedenfor



Figur 2 – Netværkssikkerhedszoner i Statens It’s standarddriftsplatform

Nedenstående tabel beskriver de enkelte sikkerhedszoner.

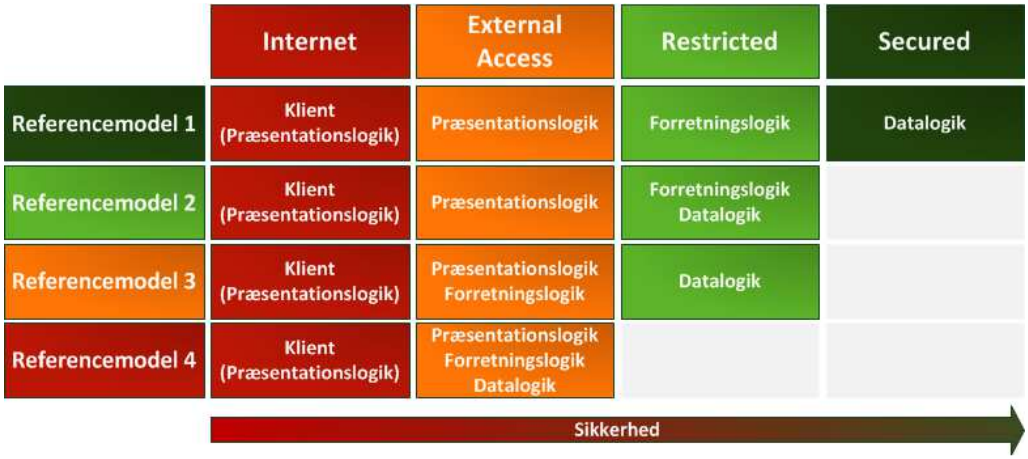
Zone	Beskrivelse	Nabozone(r)
Internet	Langt størstedelen af slutbrugere i denne zone er ikke-autentificerede og uidentificerbare.	External Access
External Access	Trafik fra internettet termineres i denne zone. Det anbefales at indholdet af denne zone holdes til et minimum. Det anbefales, at forretningsdata ***ikke*** lægges i denne zone.	Internet Client LAN Restricted Management
Client LAN	Inden for denne zone tilslutter medarbejdere deres enheder. Det anbefales, at der ikke lægges andet end klient enheder og andet perifært udstyr i denne zone.	External Access Internal Access Management
Internal Access	Denne zone kan sidestilles med zonen External Access og har til formål at separere zonen Client LAN fra interne systemer. Det anbefales, at forretningsdata ***ikke*** lægges I denne zone.	Client LAN Restricted
Restricted	For at få adgang til denne zone skal en slutbruger eller system have været igennem External Access eller Internal Access samt tilfredsstille alle sikkerhedsmæssige krav. Det anbefales, at forretningsdata samt præsentationslogik ***ikke*** lægges i denne zone.	External Access Internal Access Secured Management
Secured	Denne zone er højt sikret med begrænset adgang og er underlagt særlige sikkerheds-mæssige krav. Det anbefales, at forretningslogik og præsentationslogik ***ikke*** lægges i denne zone.	Restricted Management
Management	Denne zone er højt sikret og er udelukkende til brug for Statens It.	External Access Internal Access Restricted Secured

3.4 Referencemodeller

Nedenstående figurer viser, hvilke referencemodeller Statens It understøtter i forhold til implementering af løsninger. Referencemodellerne er baseret på forskellige systemarkitekturer og deres sammenhæng til de forskellige netværkssikkerhedszoner Statens It anvender.

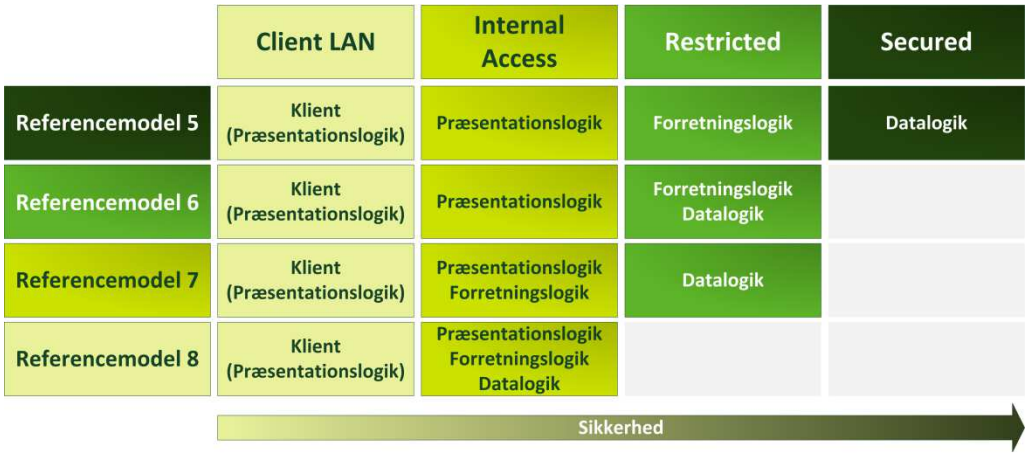
Figur 3 beskriver placeringen af logiske arkitekturlag i netværkssikkerheds-zoner for fire referencemodeller for eksternt vendte løsninger.

Referencemodellerne uddybes i underbilag A) Referencemodeller for løsninger i Statens It's standarddriftsplatform.



Figur 3 - Matrice med referencemodeller for eksternt vendte løsninger

Figur 4 beskriver placeringen af logiske arkitekturlag i netværkssikkerheds-zoner for fire referencemodeller for internt vendte løsninger. Referencemo-dellerne uddybes i underbilag A) Referencemodeller for løsninger i Statens It's standarddriftsplatform.



Figur 4 - Matrice med referencemodeller for internt vendte løsninger

Statens It anbefaler implementering af løsninger efter referencemodel 1 og referencemodel 5. Anbefalingen sker da der ønskes den højeste grad af sikkerhed som sikkerhedsaksen viser.

3.4.1 Autentificering ved brug af supporting services

Nedenstående tabeller viser, hvilke supporting services til autentificering, Statens It stiller til rådighed for forretningslogiklaget i de forskellige referencemodeller.

De øvrige supporting services er som udgangspunkt tilgængelige i alle sikkerhedszonerne og beskrivelsen af supporting services findes i afsnit 5 Supporting services.

3.4.1.1 *Supporting services til autentificering - eksterne løsninger*

Supporting Services	Referencemodel 1	Referencemodel 2	Referencemodel 3	Referencemodel 4
RADIUS	X	X		
To-faktor autentificering	X	X	X	X
Active Directory	X	X		

3.4.1.2 *Supporting services til autentificering - interne løsninger*

Supporting Services	Referencemodel 5	Referencemodel 6	Referencemodel 7	Referencemodel 8
RADIUS	X	X	X	X
To-faktor autentificering	X	X	X	X
Active Directory	X	X	X	X

Såfremt ingen af ovenstående referencemodeller kan anvendes, skal det aftales med Statens It, hvorledes løsningen implementeres.

4 Driftsplatform

Driftsplatformen består af en klientplatform og af en serverplatform samt en række basisapplikationer. Disse er beskrevet i de følgende afsnit.

4.1 Klientplatforme

I følgende afsnit behandles klientplatforme, som i denne sammenhæng afgrænses til at være den fysiske eller logiske enhed, hvorfra afvikling af klientapplikationer finder sted.

4.1.1 Webkontoret

Webkontoret er en central del af statens it-arbejdsplads og er derved den fremtidige måde hvorpå Statens It leverer klientapplikationer til slutbrugerne. Udrulning af Statens it-arbejdsplads sker i regi af et projekt, der ved udgangen af 2013 er gennemført, hvorved alle kunder hos Statens It vil have adgang til løsningen.

Webkontoret baserer sig på Citrix XenApp teknologien og gør det derfor muligt at afvikle klientapplikationer inde i Statens It's datacenter. Webkontoret afvikles på gældende Microsoft Windows Server operativsystem. Klientapplikationer, der installeres på Webkontoret, skal virtualiseres ved brug af Microsoft Application Virtualization (App-V).

Webkontoret er den platform, tredjepartsleverandører skal udvikle klientapplikationer til. Trejdepartsleverandørers adgang til standarddriftsplatformen sker ligeledes gennem webkontoret.

4.1.2 Standard pc

For at tilgå Webkontoret vil slutbrugere i forbindelse med udrulningen af Statens it-arbejdsplads blive udstyret med en bærbar pc, der er indkøbt efter gældende cirkulære om indkøb i staten. Den bærbare pc vil være med det gældende Microsoft Windows-operativsystem.

Såfremt det ikke er muligt at afvikle en given klientapplikation i Webkontoret, er der mulighed for, at denne installeres lokalt på standard pc'en. Distribution vil ske ved den gældende Microsoft System Center Configuration Manager.

4.1.3 Bring Your Own Device (BYOD)

For at imødegå behovet for anvendelse af andre enheder end standard pc, understøtter Statens It brugen af tablets, smartphones og lignende enheder. Webkontoret er tilgængeligt, såfremt enheden, hvorfra det tilgås, har internetforbindelse samt en Citrix Receiver installeret.

4.2 Serverplatformen

Statens It har med etableringen af et datacenter skabt en driftsstabil og kraftfuld platform for serverkonsolidering på en virtuel platform.

Denne platform stiller en fleksibel infrastruktur til rådighed for etablering af servere, men det udfordrer også serverbegrebet som en fysisk enhed. En server hos Statens It er ikke længere en fysisk enhed.

En virtuel server er fleksibel i placering og ressourcetildeling, men begrænset i forhold til den vært, den ligger på løsninger, der skal leve på en virtuel platform, skal ikke bestykkes, som man ville gøre det på en fysisk platform, hvilket er vigtigt at holde sig for øje, når man som tredjepartsleverandør eller kunde stiller ressourcekrav til en løsning. Statens It har defineret en standardserver, som er konfigureret efter, hvad der erfaringsmæssigt har vist sig at være de bedste valg i datacenteret. Konfigurationen er nøje beskrevet i underbilag B) Standardserverkonfiguration i Statens It's standarddriftsplatform, som opdateres løbende med udviklingen i driftscenteret. Statens It standardservere er enten konfigureret med gældende version af Microsoft Server-operativsystem eller Redhat Enterprise Linux-operativsystem jf. de interne teknologivalg for de to operativsystemer.

Afviger anbefalingen fra tredjepartsleverandøren fra dette, og er der ingen mulighed for skalering over flere instanser, skal Statens It og tredjepartsleverandøren i samråd finde den bedste løsning. Det er op til kunden at imødekomme dette krav.

4.3 Basisapplikationer

I Statens It's standarddriftsplatform tilbydes følgende basisapplikationer, som danner grundlag for kundernes løsninger.

4.3.1 Database

Statens It understøtter følgende databasesystemer på standarddriftsplatformen:

- Microsoft SQL Server
- MySQL Database
- Oracle Database
- PostgreSQL Database System

Nye systemer etableres i overensstemmelse med de gældende teknologivalg.

4.3.2 Webserver

Statens it understøtter følgende webserverløsninger på standarddriftsplatformen:

- Apache HTTP Server
- Microsoft Internet Information Server

Nye systemer etableres i overensstemmelse med de gældende teknologivalg.

4.3.3 Content management system (CMS)

Statens It understøtter følgende Content Management Systemer på standarddriftsplatformen:

- Drupal

- Microsoft SharePoint
- SiteCore CMS

Nye systemer etableres i overensstemmelse med de gældende teknologivalg.

4.4 Standard services

Udover basisapplikationerne tilbydes der drift af følgende rammesystemer. Her har Statens it opbygget kompetencer til drift.

Der pågår til stadighed et arbejde med at udbygge udbuddet af de standard services, som stilles til rådighed for kunderne.

4.4.1 Elektronisk sags- og dokumenthåndtering (ESDH)

Statens It understøtter i stort omfang drift af elektronisk sags- og dokument-systemer. I stor skala har Statens it driftsansvaret for:

- cBrain F2
- ScanJour Captia
- Software Innovation Public 360°

Nye løsninger etableres i overensstemmelse med de gældende teknologivalg.

5 Supporting services

Supporting services er komponenter, som stilles til rådighed for løsninger på Statens It's standarddriftsplatform efter de gældende teknologivalg.

5.1 Autentificering

Statens It's løsninger til autentificering er til rådighed for interne systemer, og nedenstående komponenter understøttes.

5.1.1 Active Directory

Statens It understøtter integreret Active Directory autentificering.

Anvendelsesområder:

- Autentificering for interne og eksterne brugere.

Standarder:

- Kerberos
- NTLMv2

Bemærkninger:

- Der kan ikke anvendes intern Active Directory-autentificering på løsninger, der er tilgængelige fra internettet. Hertil kan anvendes RADIUS eller to-faktor-autentificering.
- Statens It tillader ikke skemaudvidelser af det interne Active Directory til brug for enkeltløsninger.
- For eksternt rettede systemer, der ikke skal anvende intern autentificering, stiller Statens It et Active Directory til rådighed. Dette Active Directory er separeret fra det interne Active Directory.

5.1.2 RADIUS

RADIUS anvendes som autentificeringsmetode for løsninger der ikke kan anvende Active Directory autentificering samt til to-faktor autentificering.

Anvendelsesområder:

- For interne såvel som eksterne løsninger kan RADIUS anvendes til autentificering af interne brugerkonti.

Standarder:

- RADIUS

Bemærkninger:

- Der kan ydermere anvendes to-faktor-autentificering ved brug af RADIUS.

5.1.3 To-faktor autentificering

Statens It understøtter to-faktor autentificering i form af SMS Passcode.

Anvendelsesområder:

- Eksterne systemer, der kræver ekstra sikkerhed ved autentificering af interne brugere.

Standarder:
- Der anvendes RADIUS ved brug af to-faktor autentificering.

Bemærkninger:
- Der understøttes to-faktor-autentificering via SMS-token eller hardware-token.

5.2 Sikkerhedskomponenter

Statens It anvender et bredt udsnit af sikkerhedskomponenter i datacenteret til beskyttelse af data og netværkstrafik.

Anvendelsesområder:
- Der anvendes antivirus/antimalware på alle servere.
- Der anvendes Intrusion Prevention System (IPS) for alle perimetreadgange til Statens It's datacenter.

Standarder:
- Se bemærkninger.

Bemærkninger:
- Af sikkerhedsmæssige årsager beskrives de løsninger, der anvendes, ikke.

5.3 Load balance / web-caching

For såvel internt som eksternt tilgængelige løsninger understøtter Statens It anvendelsen af load balancing samt web-caching.

Load balancing er en metode til at fordele trafik fra klienter mod to eller flere front end-servere og således optimere svartider, throughput og belastning på løsningen.
Web-caching er en metode til at optimere trafik fra klienter mod en eller flere webservere og således optimere svartider på løsningen.

Anvendelsesområder:
- Load balance og web-caching kan anvendes både til internt og eksternt tilgængelige løsninger.
- Der kan anvendes SSL offload, således at eksempelvis webservere ikke skal håndtere tung kryptering af trafik.

Standarder:
- Typisk anvendes HTTP og HTTPS som transportprotokoller. Andre protokol-standarder kan anvendes med forbehold.

Bemærkninger:
- Statens It understøtter kun Load Balance ved hjælp af hardwareappliance.

5.4 Mail og kalender

Statens It's fælles mailløsning baseres på Microsoft Exchange og en central antispam-gateway med antivirus-check.

Anvendelsesområder:

- Mail, kalender, kontaktpersoner og opgavestyring via Outlook, webmail og ActiveSync.
- Mail relay fra godkendte servere via den centrale antispamløsning.

Standarder:

- ESMTP og SMTP.
- MAPI, POP3, IMAP4, HTTPS og ActiveSync.

Bemærkninger:

- Klienter, der understøtter OutlookAnywhere, https og ActiveSync, kan kommunikere fra internet til Exchange.
- Klienter der kun understøtter protokollerne POP3 og IMAP 4 skal placeres i datacentret.

5.5 Backup / Restore

Statens It's standard for backup af løsninger i standarddriftsplatformen er baseret på markedsanerkendt backupsystem. Standard backup anvendes til Disaster Recovery og backupprocedurerne er således ikke indrettet for at imødegå utilsigtede brugerfejl.

Kunden instruere gennem driftsvejledningen Statens it i hvilke data der skal backes up samt instruerer i hvordan systemkomplekset skal reetableres.

Det er derfor op til kunden at klassificere systemets data og definere den backuppolitik, der skal anvendes på systemets data. At klassificere data betyder, at man som organisation vurderer, hvor stor betydning data har for organisationens virke. Jo større betydning data har for organisationens virke, des større krav til sikkerhed, backup og restore skal der stilles til systemet.

Her er det vigtigt også at forholde sig til restore, da den tid, hvormed data genskabes efter nedbrud, vil have større eller mindre betydning for organisationens virke. Såfremt man vil sikre sig mod datafejl, enten menneskelige eller systemgenererede, er det vigtigt at forholde sig til, hvor langt tilbage i tiden, man vil kunne rulle tilbage, samt med hvilken præcision.

Alle disse forhold skal gøres til genstand for dialog med Statens It, da det vil have indflydelse for afregningen af systemet. Backup ud over standardbeskrivelsen er at betragte som tilkøb.

Statens It’s standard backuppolitikken er beskrevet i underbilag C) Backuppolitik i Statens It’s standarddriftsplatform.

5.6 Overvågning

Statens It overvåger i dag alle komponenter i infrastrukturen. Denne basisovervågning består af teknisk overvågning på bl.a.

- Netværk

- Server services
- VMware
- SAN og andre disksystemer
- Temperaturer i datacenter
- Fysiske servere

Indeholdt i basisovervågning er også Statens It's overvågning af de shared services, der tilbydes kunderne set ud fra en funktions-/applikationsvinkel.

- Mail og kalender
- AD
- Webkontoret

Såfremt ovenstående overvågning ikke er fyldestgørende, skal yderligere overvågning aftales med Statens It.

5.7 Andre services

5.7.1 Domain Name System (DNS)

Statens It stiller DNS til rådighed for løsninger, interne såvel som eksterne, til brug for navneopslag, både for interne og eksterne opslag.

5.7.2 Time Services

Statens It stiller Time Services (NTP) til rådighed for løsninger, interne såvel som eksterne, til brug for sikker og stabil tidssynkronisering. Statens It har to fysiske NTP-servere, der synkroniserer tid med den officielle danske NTP-pulje.

5.7.3 Virtual Private Network (VPN)

Statens It understøtter VPN adgang til Statens It's standarddriftsplatform fra enheder udleveret af Statens It. For andre platforme skal det aftales specifikt med Statens it.

Anvendelsesområder:

- Adgang til Statens It's datacenter via sikker VPN forbindelse.

Standarder:

- Statens It anvender Cisco anyConnect som standard for VPN forbindelser.

Bemærkninger:

- Der anvendes to-faktor autentificering ved anvendelse af VPN.

6 Teknologivalg

Statens It's kerneforretning er baseret på sikker og stabil drift, hvorfor der i videst muligt omfang vælges modne teknologier og løsninger. Statens It's overordnede arkitekturprincipper dikterer dette mere direkte i princippet om "Teknologivalg".

Det anbefales tredjepartsleverandører at imødegå dette krav om modenhed og ikke basere løsninger på "bleeding edge"-teknologier på standarddriftsplatformen.

For tredjepartsleverandøren vil de services, som løsningen er afhængig af, skulle afklares i forhold til de individuelle teknologivalg, således, at der er overensstemmelse med kravene fra leverandøren og den driftsplatform, Statens It leverer, både på implementeringstidspunktet og i produktets afskrivningsperiode.

Bilag 11 foreskriver de teknologivalg, der er truffet i etableringen af standarddriftsplatformen. Teknologivalg er beskrevet samlet i underbilag D) Teknologi.

Ved identificerede uoverensstemmelser skal kunden tredjepartsleverandøren tage kontakt til Statens It.

7 Revisionshistorik

Revisions-dato	Version	Kort resumé	Afsnit	Forfatter
Januar 2014	1.0	Præcisering af formål med bilag 11	Afsnit 1.1, formål.	Servicesekretariatet, Statens It