Fiktivmyndigheten

2021-04-07

Nulägesbeskrivning

Fiktivmyndighetens IT-miljö

Fiktivmyndigheten

Innehållsförteckning

1 Om detta dokument 2
2 Om Fiktivmyndigheten 2
3 Allmänt om IT-miljön 3
4 Datacenter 4
5 Hårdvara 4
6 Kommunikation 5
7 Systemprogramvaror 7
8 Systemunderhåll 8
9 Kontorsstöd 8
10 Volymer 9

1 Om detta dokument

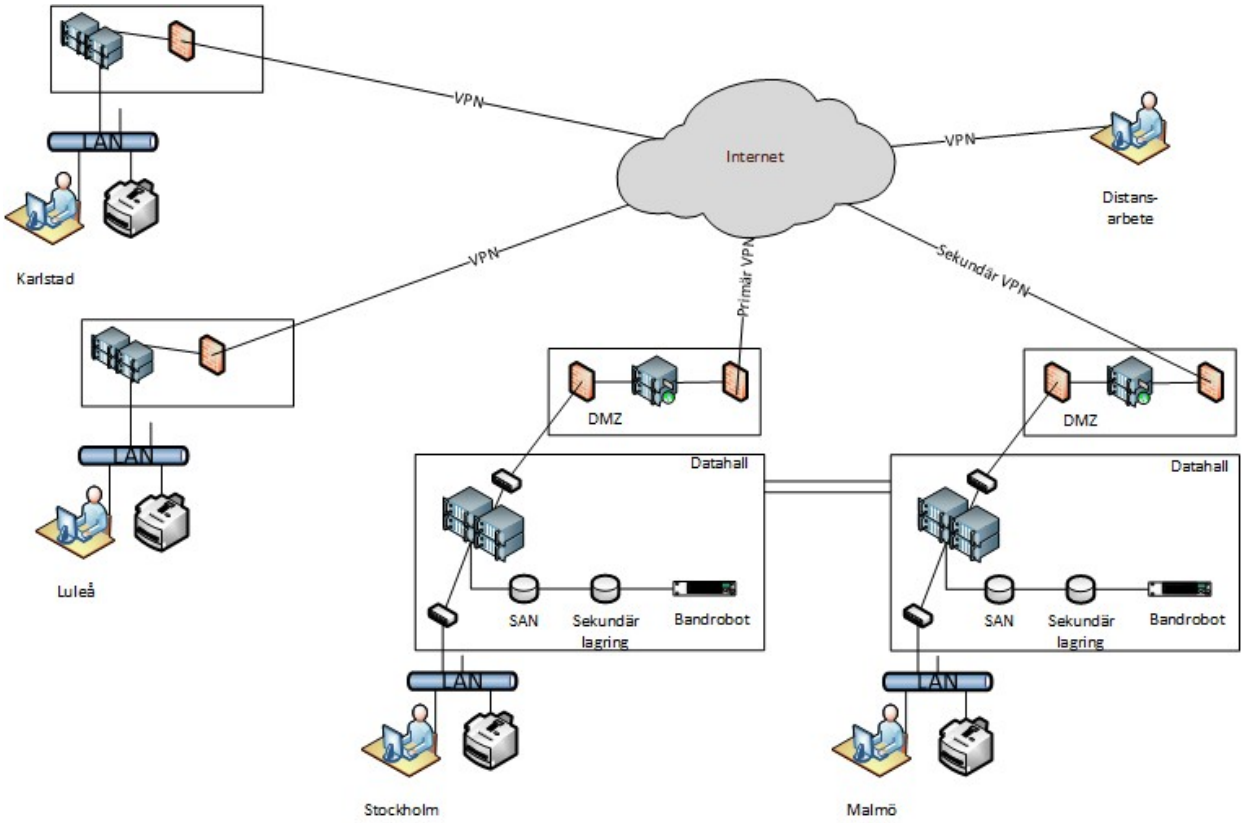
Detta dokument avser att ge en översiktlig bild av hur Fiktivmyndighetens IT-miljö ser ut vid aktuellt dokumentdatum och ska vara ett underlag för dialog och hjälp vid upphandling och avrop av IT-system till Fiktivmyndigheten.

2 Om Fiktivmyndigheten

Fiktivmyndigheten har kontor i Stockholm, Luleå, Karlstad och Malmö. Det är totalt ca 700 anställda fördelat på 350 i Stockholm, 20 i Luleå, 80 i Karlstad samt 250 i Malmö. IT-avdelningen har ca 25 anställda. Fiktivmyndigheten behandlar i dagsläget personuppgifter och sekretessbelagd information men ingen information som är säkerhetsklassificerad. Risk- och sårbarhetsanalyser för verksamheten genomförs regelbundet. Även en katastrofplan som uppdateras regelbundet finns.

3 Allmänt om IT-miljön

3.1 Schematisk bild över IT-miljön



3.2 Övergripande beskrivning

Fiktivmyndighetens verksamhet är informationsintensiv och hanterar stora mängder data. För att säkerställa hög tillgänglighet på IT-systemen finns två datacenter för verksamhetssystemen samt två mindre serverrum för utskriftsservrar och filservrar.

Kontoren är utrustade med trådbundna som trådlösa lokala nätverk. Luleå och Karlstad är sammankopplade med Stockholm och Malmö via VPN över internet. Datacentren i Stockholm och Malmö är sammankopplade med separata förbindelser.

Fiktivmyndigheten har en standardiserad klientplattform som används av merparten av alla anställda. Utöver detta finns ytterligare ett antal klienter i verksamheten som inte använder den myndighetsgemensamma klientplattformen. Samtliga anställda har en mobiltelefon.

För utskrifter använder Fiktivmyndigheten multifunktionsskrivare och en utskriftstjänst som innebär att utskrifterna köas i en myndighetsgemensam utskriftskö.

All IT-utrustning livscykelhanteras över fem år vilket innebär att utrustningen byts ut mot ny motsvarande utrustning efter ca fem år.

4 Datacenter

Fiktivmyndigheten har två datacenter placerade i Malmö respektive Stockholm.

Datacentren är prefabricerade datacenter med skyddsklass 2 enligt SSF 200, låsklass 3 enligt SS 3522 samt brandklass enligt SS/EN 1047-2. Datacenter är utrustade med klimatanläggning och har dubbla redundanta strömförsörjningar samt UPS och reservkraft i form av dieselaggregat. Dieselaggregat är dimensionerat för 24 timmars drift.

Datacentren är speglade och är samtidigt aktiva vilket innebär att lasten fördelas mellan bägge datacentren.

I vardera datacenter finns servrar för verksamhetssystem, test och utveckling. Test och utvecklingsservrar är på båda orterna placerade i separata rack i en avgränsad zon av vardera datacenter.

Utöver dessa stora datacenter finns även mindre serverrum i Luleå och Karlstad. I dessa finns servrar för fillagring och utskrift. Filer kopieras en gång per dygn till Stockholm och Malmö.

SAN, utrustning för säkerhetskopiering samt kommunikationsutrustning för servrar och lagringsutrustning är placerade i datacentren i Stockholm och Malmö.

5 Hårdvara

5.1 Servrar

Servrar i datacentren i Stockholm och Malmö är rackservrar. Samtliga rackservrar har hög redundans i form av dubbla kraftaggregat, speglade systemdiskar samt dubbla nätverks- och SAN-anslutningar och använder SAN för lagring. Stockholm och Malmö har lika många servrar. Mindre servrar har dubbla 1 Gb/s Ethernet och dubbla 16 Gb/s Fibre Channel, större servrar har dubbla 10 Gb/s Ethernet och dubbla 32 Gb/s Fibre Channel.

Servrar i Luleå och Karlstad är rackservrar med hårddiskar monterade i separata diskkabinett och dubbla 10 Gb/s Ethernet.

Servrar är från flera olika varumärkesägare.

Installation, konfigurering, uppdatering, uppgradering, licenshantering, övervakning m.m. av servrarna sköts av Fiktivmyndighetens IT-avdelning.

5.2 Lagring och säkerhetskopiering

Samtliga servrar i datacentren i Stockholm och Malmö lagrar data i ett SAN där all prioriterad data synkroniseras mellan datacentren.

Utrustning för sekundärlagring som främst används för säkerhetskopiering finns placerad i båda datacentren.

Utrustning för säkerhetskopiering som finns i båda datacentren består av produkter från flera varumärkesägare och licensgivare. All säkerhetskopiering görs i datacenter i Stockholm med utrustningen i Malmö som reserv.

För att minimera den tid som verksamhetssystemen påverkas av säkerhetskopieringen sker den i två steg. Först en snabb kopiering mellan SAN och sekundärlagring. Därefter kopieras allt från sekundärlagring till band med hjälp av en bandrobot.

Säkerhetskopiering av all verksamhetskritisk data sker automatiskt efter ett schema bestående av dels total säkerhetskopiering och dels säkerhetskopiering av förändringar sedan föregående kopiering.

5.3 Klientdatorer

Samtliga anställda har en bärbar dator samt extern bildskärm, tangentbord och mus. Klientdatorer är från flera olika varumärkesägare.

5.4 Telefoner

Fiktivmyndighetens anställda har mobiltelefoner fördelade 50/50 på IOS och Android. Förutom telefonfunktionerna används de främst för e-post, kalender och webb.

Medarbetarna har även softphone. I de flesta mötesrum finns det konferenstelefoner.

5.5 Skrivare

Fiktivmyndigheten har en central utskriftsserver och användarna har tillgång till multifunktionsskrivare (MFP) som fungerar som nätverksskrivare, kopiator och skanner.

MFP nyttjar funktionerna Follow Me Print och Secure printing vilket innebär att utskriften ligger kvar i skrivarkön och tas ut på valfri MFP efter autentisering med kort. Drivrutin är installerad i samtliga klientdatorer. MFP ligger på eget VLAN.

6 Kommunikation

6.1 Datacenter

I datacentren finns nätverksväxlar som sköter kommunikation mellan servrar och LAN i datacentren samt mellan datacenter. Nätverk är redundant och har både 1 och 10 Gb/s Ethernet. Ett redundant SAN består av blocklagring och Fibre Channel växlar och har både 16 och 32 Gb/s Fibre Channel. Dessutom finns lastbalanserare vars uppgift är att fördela lasten mellan datacentren.

Nätverksväxlar i Stockholm är från en varumärkesägare och från en annan varumärkesägare i Malmö.

6.2 Internet

För att Fiktivmyndigheten inte ska vara beroende av enbart en ISP är kontoren i Stockholm, Karlstad och Luleå anslutna mot en ISP medan kontoret i Malmö har en annan ISP. Alla internet-anslutningar termineras hos Fiktivmyndigheten med routrar som ägs av ISP. Fiktivmyndigheten har fulla administrativa rättigheter till ISP:s routrar.

Anslutningen mot internet är redundant med BGP mellan router i Stockholm och Malmö.

All trafik från Karlstad och Luleå, inklusive trafik till internet, skickas i VPN-tunnel primärt till Stockholm och med Malmö som sekundär anslutning.

Användare i Malmö går primärt ut på internet via anslutning i Malmö med Stockholm som sekundär anslutning.

Karlstad och Luleå har ”Bastjänst A: Internetaccess symmetrisk”, avropad från ramavtalet ”Kommunikationstjänster” vilket innebär att följande funktioner ingår:

- Symmetrisk anslutning inom Sverige
- Bandbredden är 200 Mb/s med obegränsad trafik
- Både IPv4 och IPv6 i Native mode
- Fast tilldelade IP-adresser mot internet
- Namnuppslagning med DNS och DNSSEC för både IPv4 och IPv6

Stockholm och Malmö har ”Bastjänst A: Internetaccess symmetrisk” med utökningar, avropad från ramavtalet ”Kommunikationstjänster” vilket innebär att följande funktioner ingår:

- Symmetrisk anslutning inom Sverige
- Bandbredden är 10 Gb/s med obegränsad trafik
- Både IPv4 och IPv6 i Native mode
- Fast tilldelade IP-adresser mot internet
- Namnuppslagning med DNS och DNSSEC för både IPv4 och IPv6
- Skydd mot överbelastningsattacker som inkluderar övervakning av nätet, skydd mot volymetriska attacker, snabb aktivering inom någon minut vid attack, släpper igenom legitim trafik, hanterar attacker upp till 100 Gb/s samt hanterar Fiktivmyndighetens samtliga publika IP-adresser.

6.3 WAN

Stockholm och Malmö är sammankopplade med fyra separata förbindelser i form av våglängder från samma operatör. Våglängderna är parvis fullständigt fysiskt separerade. Två förbindelser används till 10 Gb/s Ethernet och de andra två används till 32 Gb/s Fibre Channel.

6.4 LAN

På varje kontor finns både trådbundet och trådlöst LAN.

Alla kontorsarbetsplatser är utrustade med ett nätverksuttag för trådbundet LAN med 1 Gb/s. Alla våningsplan har fyra accesspunkter per våningsplan för trådlöst LAN. Accesspunkter strömmatas med eget nätaggregat. I konferensrum finns endast trådlöst LAN.

Fastighetsnätets kablage är kategori 6. I korskopplingsrum på varje våningsplan ansluts de trådbundna nätverksuttagen mot korskopplingspaneler varifrån de patchas mot nätverksväxlar. Varje våningsplan har ett korskopplingsrum. Även accesspunkterna för trådlöst LAN ansluts mot nätverksväxlarna i korskopplingsrum på samma våningsplan. Dessa nätverksväxlar ansluts i sin tur via fiber, med 10 Gb/s, mot en central nätverksväxel på respektive orts datacenter eller serverrum.

Fiktivmyndigheten har standardiserat korskopplingsrummen med 24-portars nätverksväxlar. Nätverksväxlar är från flera olika varumärkesägare. Samtlig utrustning är fullt övervakningsbar och stöder alla normalt förekommande öppna standarder, dock inte PoE.

Autentiseringen till trådlöst LAN sker med 802.1X. Det finns ett gästnätverk för gäster som behöver tillgång till internet genom ett separat SSID.

Samtliga anställda kan arbeta på distans via VPN-uppkoppling.

6.5 DMZ

Fiktivmyndigheten har ett DMZ i Stockholm och ett i Malmö i vilket servrar för VPN, DNS, e-post och extern webb finns.

Brandväggar mot internet och LAN är fysiskt separerade. Nätverksväxlarna i DMZ är fysiskt separerade från övriga LAN. Separat IDS finns. Brandväggar mot internet är från en varumärkesägare och brandväggar mot LAN är från en annan varumärkesägare.

Servrar för DNS och DNSSEC är baserade på Linux och BIND 9.

Servrar för VPN är baserade på Linux och OpenVPN 2.

Allt på DMZ har dubbla IP-stackar, IPv4 och IPv6.

6.6 Telefoni

Fiktivmyndigheten har en abonnentväxel i Stockholm med anslutning till det publika telenätet.

Myndigheten har följande telefonifunktioner: kontaktcenter, automatisk samtalshantering, automatisk telefonist, talsvar, callback, röstbrevlåda, hänvisning och telefonkatalog.

På kontoret i Stockholm finns telefonister som besvarar samtal för samtliga orter.

Samtliga medarbetare har både en mobil anknytning och en softphone anknuten till abonnentväxeln. Flertalet mötesrum har en anknytning i abonnentväxeln.

Kontaktcenter har licens för 50 samtidiga agenter för service mot externa kunder.

Medarbetarna använder nästan uteslutande mobiltelefoner i sitt dagliga arbete men myndigheten ser softphone och anknytningarna i växeln som viktiga av säkerhetsskäl och som ett tillförlitligt reservalternativ till mobiltelefonin.

7 Systemprogramvaror

7.1 Operativsystem servrar

De fysiska servrarna i datacentren respektive serverrummen körs med följande operativsystem:
Red Hat Enterprise Linux 7
Microsoft Windows Server 2012
Microsoft Windows Server 2016

På de fysiska servrarna med Linux och Windows Server finns ofta virtualiseringsprogramvara, VMware vSphere 6 för Windows Server och KVM för Linux. På de virtuella servrarna används samma versioner av Windows Server och Linux som på fysiska servrar.

7.2 Operativsystem klienter

På klienterna används följande operativsystem:
Microsoft Windows 10 (standardiserad klientplattform)
Ubuntu Linux 18.04

7.3 Databashanterare

De databashanterare som används är:
Microsoft SQL Server 2017
PostgreSQL 11
MariaDB 10

8 Systemunderhåll

8.1 Övervakning
Fiktivmyndigheten har Icinga 2 som övervakningssystem som regelbundet kontrollerar status på och tar emot larm från IT-miljöns hårdvaror och programvaror. Övervakningssystemet kan skicka kritiska larm vidare till systemadministratörerna via e-post och SMS.

8.2 Distributionsprogramvara
För klientdatorer med Windows sker distribution av operativsystem, drivrutiner och applikationer via central policy med hjälp av Microsoft System Center Configuration Manager. För klientdatorer med Linux administreras dessa lokalt av användarna.

8.3 Virusskydd
Samtliga servrar och klienter har aktivt virusskydd som styrs via central policyhantering.

8.4 VPN
För kommunikation mellan kontor och för arbete på distans över internet används OpenVPN 2.

9 Kontorsstöd

9.1 Katalogtjänst
För att användaren ska kunna komma åt sin arbetsmiljö krävs tillgång till en personlig användaridentitet. Beroende på vilken avdelning användaren tillhör får användaren med automatik åtkomst till standardapplikationer, övriga applikationer, lagringsarea såsom hemkatalog samt gemensam fillagringsyta. För hantering av rättigheter och styrning används Microsoft Active Directory. Samtliga klientdatorer autentiserar mot Active Directory.

För att höja säkerheten nyttjar Fiktivmyndigheten Active Directory Certificate Services för dator- och användarautentisering.

9.2 Webb
Både extern webb och intranät är byggda med Linux, nginx 1 och Drupal 8.

9.3 E-postserver
Som e-postserver används Microsoft Exchange 2016.

9.4 Kontorsprogram
Alla klientdatorer har normala kontorsprogramvaror och webbläsare.

9.5 Videokonferens
Samtliga klientdatorer och mobiltelefoner har programvara för videokonferens för både intern och extern kommunikation.

Fiktivmyndigheten

10 Volymer

I denna tabell finns en sammanställning av volymer för Fiktivmyndigheten.

Objekt	**Stockholm**	**Malmö**	**Karlstad**	**Luleå**
Antal anställda	350	250	80	20
Antal våningsplan	6	4	2	1
Rackserver 1G E / 16G FC	96	96		
Rackserver 10G E / 32G FC	192	192		
Rackserver 10G E			2	2
Blocklagring	1	1		
Fibre Channel växel	2	2		
Diskkabinett			1	1
Bandrobot	1	1		
Bärbar PC med Windows	340	240	80	20
Bärbar PC med Linux	10	10		
Abonnentväxel	1	1		
Mobiltelefon med IOS	175	125	40	10
Mobiltelefon med Android	175	125	40	10
Multifunktionsskrivare	12	8	4	2
Lastbalanserare	1	1		
Nätverksväxel korskoppling	18	12	4	2
Nätverksväxel datacenter	2	2		
Nätverksväxel DMZ	2	2		
Nätverksväxel serverrum			1	1
Accesspunkter trådlöst LAN	24	16	8	4
Brandvägg	2	2		
Fysisk server med Windows Server 2012	10	10		
Fysisk server med Windows Server 2016	10	10	2	2
Fysisk server med Linux	28	28		
Fysisk server med Windows + VMware	80	80		
Fysisk server med Linux + KVM	160	160		