VGR:s IT-miljö
Datum

VGRs IT-miljö

November | 2025 | rev.1

VÄSTRA GÖTALANDSREGIONEN

Förord

Västra Götalandsregionen (VGR) är en av Sveriges största organisationer och har därmed även en omfattande och komplex IT-miljö.

Detta referensmaterial syftar till att ge en introduktion till och överblick över VGR:s IT-miljö och de tekniska komponenter, tjänster och lösningar som tillsammans utgör dess underliggande och möjliggörande IT-infrastruktur. Materialet fokuserar på tekniska förmågor men inkluderar även något om förvaltning och styrning som kan vara bra att känna till.

Innehållet ger ingen fullständig bild av helheten och går heller inte ner på detaljnivå, utan är tänkt som orientering och referens för medarbetare och andra intressenter som behöver få en introduktion och överblick över IT-miljön.

Detta dokument kan användas som referensdokument vid dialog med leverantörer och andra externa intressenter i syfte att skapa en bättre förståelse för den IT-miljö som den upphandlade lösningen kommer att bli en del av.

Då faktiska förhållanden förändras löpande kommer nya versioner av detta dokument publiceras regelbundet. Informationen i dokumentet ska därför enbart ses som ett orienterande referens- och informationsmaterial och kan inte användas som underlag för avtalsgrundande krav.

Läsaren av detta dokument förutsätts vara tekniskt bevandrad.

Vid frågor eller behov av en närmare dialog runt något specifikt område eller någon annan aspekt kring VGR:s IT-miljö, kontakta någon av personerna nedan.

Trevlig läsning!

Noak Eldh
Chefsarkitekt, koncernstab digitalisering
E-post: noak.eldh@vgregion.se

Innehåll

Arbetsplats

Produktområde Arbetsplats ansvarar för de regionala verktyg och processer som möjliggör en central hantering av klienter och utrustning som kan betraktas som användarnära.

Arbetet stöds av marknadsledande verktyg och lösningar som tillsammans erbjuder förmåga att hantera mycket stora mängder klienter och användare.

Den stora mängden klienter gör att vi alltid strävar efter standardisering och skapar förutsättningar för hög säkerhet där så krävs.

Samtidigt så finns förmågan att erbjuda en mer personligt anpassad enhet i de fall arbetsuppgifterna kräver och tillåter detta. Användning av standardiserade verktyg och processer ger också möjlighet till nationellt samarbete med andra regioner och kommuner.

Området arbetar löpande på att optimera hantering av enheter och användare genom att möjliggöra automation och att administration så långt som möjligt hanteras i eller nära den ansvariga verksamheten.

Produktområdet innefattar idag följande produkter:

- **Desktop**
  Hantering av VGR-ägda datorer

- **Mobil**
  Hantering av mobila enheter

- **Print**
  Hantering av regionala tjänster för utskrift

- **VDI**
  Hanterar virtuella datorer och applikationer

Desktop

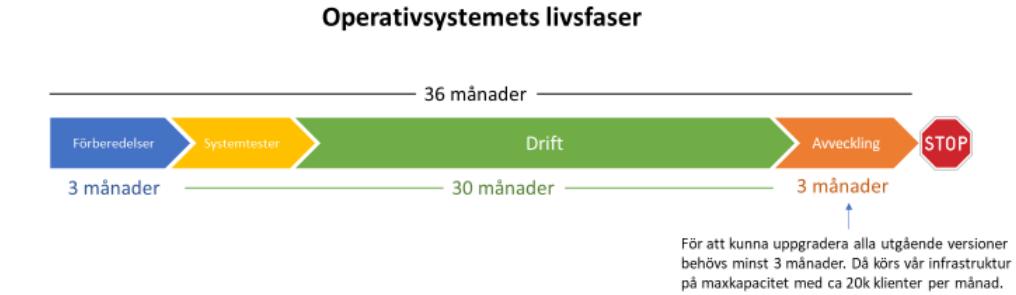
Produkten desktop omfattar de tjänster och den stödjande teknik som krävs för att leverera och hantera de c:a 60.000 datorer som ägs av och används inom VGR.

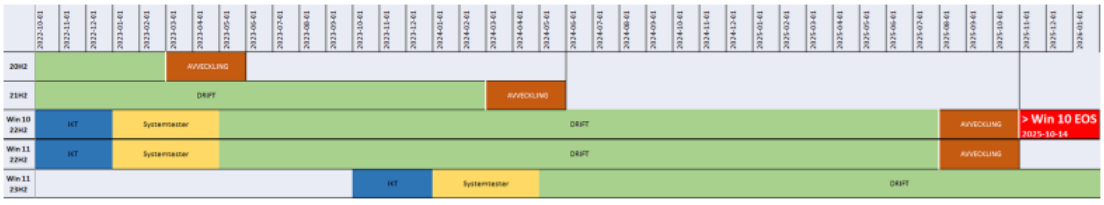
I produkten ingår infrastruktur och verktyg för att hantera:

- Distribution av operativsystem
- Distribution av applikationer
- Distribution av uppdateringar till applikationer och operativsystem
- Konfiguration av operativsystemsinställningar
- Konfiguration av webbläsare

De operativsystem som hanteras idag är Windows Enterprise x64 (XXH2) enligt Microsoft fastställda livscykel.

När Microsoft släpper en ny version går startskottet för arbetet med att förbereda vår infrastruktur för distribution av den nya versionen. Efter ungefär 3 månader görs den nya versionen tillgänglig för validering i form av system- och applikationstester, varefter den godkänns för distribution till fysiska och virtuella datorer.





Operativsystem och applikationer distribueras och hanteras via Microsoft MEMCM samt ett nationellt utvecklat gränssnitt mot MEMCM för tekniker.

Mobil

Produkten Mobil omfattar de förmågor och tjänster som hanterar Västra Götalandsregionens tjänstetelefoner och surfplattor.

Organisationen kravställer att all ägd mobil utrustning skall vara centralt hanterad. Detta sker i huvudsak genom plattformen Microsoft Intune. Även de arbetsverktyg som erbjuds på utrustningen i form av appar & tjänster skall vara centralt hanterade.

Målgrupp

Inom produkten hanteras primärt mobila enheter som nyttjas av medarbetare inom VGR, men även andra användargrupper förekommer. Exempel på användargrupper som nyttjar produktens erbjudanden inkluderar:

- Vårdpersonal
- Administrativ personal
- Förtroendevalda och politiker
- Patienter

Plattformar

- Android Enterprise
- iOS / iPadOS

Stödjande verktyg

- Microsoft Intune
- Apple Business Manager
    - Apple Automated Device Enrollment
    - Apple Volume Purchase Program
- Samsung Knox Mobile Enrollment
- Google Zero Touch
- Managed Google Play
- Sysman (Inera, Eklient)

Förmågor

Förmågorna beskriver de funktionella delar som tillsammans möjliggör hantering och leverans av de mobila lösningarna.
Produkten erbjuder centraliserade lösningar som tillgodoser verksamhetens behov av en säker, flexibel och enhetlig hantering av mobil utrustning.

- Enhetskonfiguration & anpassning
- Livscykelhantering
- Säkerhet & efterlevnad

- Applikationshantering
- Dataskydd för app
- Support & fjärråtgärder
- Användarstöd & självservice
- Spårbarhet & rapportering

Leverabler

Varje leverabel baseras på gemensam teknik och säkerhetsnivå, men anpassas efter användningskontext och behov i verksamheten.

- Mobil utrustning – personlig (för enskild användare)
- Mobil utrustning – delad (för gemensamt bruk inom arbetsgrupp)
- Mobil utrustning – kiosk (för fasta verksamhetsstationer)
- Mobil utrustning – patient (för tillfälligt bruk av patienter)

Stödjande produkter och plattformar

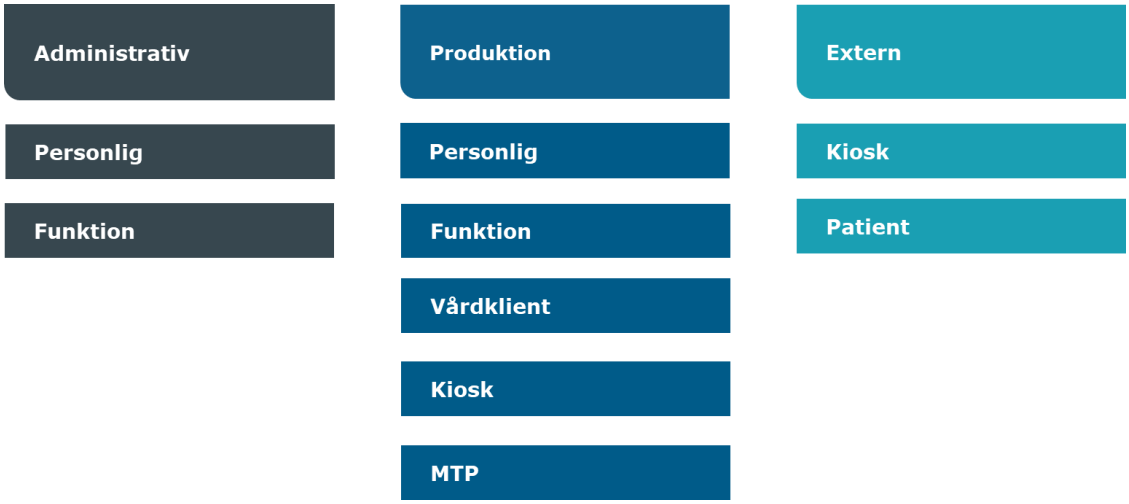
- Applikationsleverans
- Produktförvaltning
- Identifiering & åtkomst
- Telefoni & meddelandetjänster
- Säker nätverksåtkomst
- Säker endpoint
- Plexus (ITSM-plattform)

Leveranser

Den mobila VGR klienten är en sammansättning av flera förmågor inom produkten, samt integrerade förmågor från andra produkter och produktområden.

Dessa förmågor och anpassningar levereras tillsammans i form av flera kategorier, även kallade *funktionsprofiler*. Utformning sker i dialog med verksamheten och utgår efter specifika funktionella behov. Avsikten är att endast testad och godkänd utrustning skall möjliggöras för varje kategori.

Idag levereras mobila enheter inom områdena **Administrativ**, **Produktion** och **Extern** som avspeglar utrustningens användare och vilka tjänster som finns tillgängliga för användaren.



Personlig

Utrustning som är knuten till en enskild medarbetare. Användaren erbjuds ett flexibelt verktyg där innehåll kan anpassas efter användarens behov och önskemål.

Funktion

Utrustning som användas av en eller flera medarbetare. Samtliga enheter inom en kategori utformas på samma sätt med målsättningen att man skall känna igen sig mellan enheter.

Vårdklient

Utrustning som används av en eller flera medarbetare. Samtliga enheter inom en kategori utformas på samma sätt med målsättningen att man skall känna igen sig mellan enheter. Kategorin är en utveckling av tidigare funktionskategori med bl.a. inloggning för åtkomst till utrustningen.

MTP

Utrustning som betraktas som, eller är tätt integrerade mot medicinsktekniska produkter knyts till en egen kategori. Vanligtvis är dessa utformade likt enheter inom Funktion.

Kiosk

Utrustning som används för enskilda behov. Vanligt förekommande i publika eller andra allmänna miljöer. Utrustningen är kraftigt begränsad och nerlåst för att endast möjliggöra avsedd funktion. Lösningen kan erbjudas i alternativ, både för anställda samt patienter.

Patient

Utrustning som nyttjas av personer som inte är anställda av regionen, vanligtvis patienter. Exempelvis låneutrustning för att delta i videosamtal.

Print

Produkten Print omfattar de tjänster och den stödjande teknik som krävs för att leverera och hantera de befintliga plattformar för utskrift som idag används inom VGR.

Samtliga produkter kopplade till utskrift skall kunna central hanteras.

Följande är de två huvudsakliga utskriftsplattformar som används inom VGR idag:

VPSX

KSD:s nya standardplattform för utskrift från leverantör Levi, Ray & Shoup Inc.

Samtliga nya införanden av system måste stödja och valideras mot denna plattform.

Denna moderna plattform kommer att ha flera nya förmågor för att kunna säkerställa VGR:s krav på säker utskrift och mobilitet, distribuerad utskrift hos externa organisationer med mera.

Den nya printplattformen kommer bland annat ha stöd för följande typer av utskrift:

- Direkt utskrift
- Säker utskrift
- Mobil utskrift
- Utskrift hos externa organisationer
- Backendutskrift
- Delegerad utskrift
- Utskrift från VDI (Virtuella Datorer)

I initialt skede så kommer enbart Säker utskrift och direkt utskrift för kontorsprogram vara godkänt då test och verifiering för att säkerställa äldre systems kompabilitet måste göras innan vi kan släppa på äldre system med dess olika typer av utskrifter.

Riktlinjer och krav för införanden av nya system fås via kontakt med VGR Krav och Test.

VGR Print

Egenutvecklad tjänst för identifiering av närliggande skrivare för standardutskrift. Tjänsten uppfyller inte dagens krav på utskrift och kommer med start under 2024 att avvecklas till förmån för den nya utskriftsplattform som etablerats. VGR Print stöder följande typer av utskrift:

- Direktutskrift

VDI

Produkten VDI omfattar de tjänster och den stödjande infrastruktur som krävs för att leverera virtuella datorer (VDI) till medarbetare både inom VGR samt hos externa aktörer såsom kommuner, privata vårdgivare med flera. VGR:s infrastruktur för virtuella datorer bygger på produkten VMware Horizon VDI software solutions.

En VDI är en virtuell dator (fjärrskrivbord) som användare kan fjärransluta till via klientapplikationen VMware Horizon Client/webb vilken möter krav på autentisering och säker kommunikation, och som kan köras på många olika typer av enheter, som till exempel dator, mobiltelefon, surfplatta eller tunn klient.

Det är möjligt att byta den klientenhet en använder för att ansluta till en och samma VDI, till exempel byta från att ansluta via en tunn klient till att använda en surfplatta. Startade applikationer och öppnade fönster på VDI:n kommer att vara igång vilket innebär att man snabbt kan fortsätta sitt arbete via den nya klientanslutningen.

En VDI från VGR består i grundutförandet av en Microsoft Windows-baserad virtuell dator med de grundläggande applikationer (t.ex. antivirus) som är gemensamma för alla datorer inom Regionen.

Befintliga varianter av VDI

Inom VGR erbjuds idag följande varianter av VDI:

Instant Clone

En "instant clone" är en VDI inte existerar när den inte används, utan skapas automatiskt först när en användare ansluter via en klient och loggar in. Den virtuella datorn finns kvar så länge den används men tas bort när användaren loggar ut eller när det gått sex timmar utan klientanslutning. Nästa gång användaren loggar in skapas en helt ny virtuell dator och cykeln upprepas.

Detta innebär att det inte är möjligt att spara någonting lokalt på datorn; lokala filer (till exempel i foldern "Nedladdade filer") och inställningar försvinner när den virtuella datorn förstörs.

Vid planering för användning av en Instant Clone bör hantering av kringutrustning beaktas, då det inte är självklart att den fungerar på samma sätt som den gör på en standard PC. Vidare kan det finnas resurs- och prestandaskillnader, exempelvis kan en applikation kräva mer minne än vad som finns tillgängligt för en standard VDI.

VDI av denna typ används av verksamheten i tjänsterna *Förenklad åtkomst vård* och *Vårdinfo Vårdval PVG* (före detta Tapir). Instant Clone kommer även att användas för att ge åtkomst till *Millennium,* VGR:s nya kärnsystem för hälso- och sjukvård, för med arbetare inom VGR och hos externa vårdgivare som har vårdavtal med VGR.

Medarbetare inom VGR ansluter primärt till denna variant av VDI via en så kallad "Sessionsdator", en VGR-anpassad tunn klient, med möjlighet att även ansluta via andra typer av klientenheter som till exempel personlig dator.

Medarbetare hos externa vårdgivare som har vårdavtal med VGR har åtkomst till VDI för *Vårdinfo Vårdval PVG* via *Sjunet* genom en lokalt installerad klientmjukvara på användarnas egna datorer. För denna type av anslutning krävs autentisering via eTjänstekort (SITHS).

Full Clone

En "full clone" är en permanent VDI som till skillnad från en "instant clone" skapas redan när den beställs, som fortsätter att existera även om användaren loggar ut och oavsett om eller hur ofta eller sällan användaren ansluter.

Detta innebär att den virtuella datorn är uppbyggd, konfigurerad och används på ett likartat sätt som en vanlig fysisk dator samt att lokala filer och inställningar bevaras även om användaren loggar ut eller endast ansluter med långa mellanrum.

VDI-variant under införande

Publicerad applikation

Det finns även möjlighet att ge fjärråtkomst åt enstaka applikationer utan att behöva tillhandahålla ett helt virtuellt skrivbord eller en hel VDI.

För användaren upplevs en publicerad applikation som om de vore installerade på den egna lokala datorn medan den i själva verket körs på en central VDI eller terminalserver och fjärrstyrs via den lokala klientapplikationen.

Denna lösning kommer att användas för att ge åtkomst till *Millennium* för medarbetare inom regionens kommuner.

Samarbetsplattformar

Inom området samarbetsplattformar hanteras regionala verktyg för det allmänna och vardagliga arbetet. Här ryms funktionerna i Office 365, som t e x Epost, samarbetsverktyget Teams, dokumenthantering i SharePoint / Onedrive och Office-applikationerna på PC.

Samarbetsplattformar rymmer också de distansmötesplattformar vi har utöver MS Teams, vilka är Cisco SMS/Webex och PEXIP som möjliggör digitala möten som idag inte kan ske i molntjänster. Här har vi också hand om AV-utrustningen i våra mötesrum som utgörs av en stor flora av videokonferensutrustning, styrpaneler, väggskärmar, kameror med mera.

Våra slutanvändare kommer i mångt och mycket åt funktionerna ovan via beställning av en sammanhållen användartjänst. Denna tjänst är tillgänglig i olika nivåer beroende på slutanvändarens behov.

När det gäller utrustning i mötesrum så har vi en process med stöttande kompetens för val av utrustning.

Samarbetsverktyg

Vision

Erbjuda moderna generella verktyg och stöd för att på ett enkelt sätt kunna producera och samarbeta med digitalt innehåll användare emellan, inom samma ekosystem.

Ge användarna de bästa förutsättningarna för att kunna utföra sina arbetsuppgifter med hjälp av våra verktyg på ett säkert sätt.

Våra tjänster resulterar i att verksamheternas vardagliga sysslor kan flyta på enkelt utan onödig administration.

Behov

Denna produkt fyller behovet att kunna skriva och hantera dokument, kalkylark, rapporter och grafer, presentationer; skicka/ta emot epost, göra kalenderbokningar; mötas och samarbeta via chatt, ljud eller video; skapa och dela videomaterial; återanvända producerat material i olika verktygen; planera och fördela uppgifter digitalt med mera.

Genom denna produkt kan vi samarbeta genom samtliga verktyg på ett sammanhållet och säkert sätt.

Målgrupp

- Alla anställda inom VGR med användartjänst
- Externa användare till viss del
- Privata vårdgivare
- Externa bolag (VGR)

- Invånare och patienter
- Externa leverantörer
- Kommuner och regioner

Nuvarande produkter

- Outlook
- Word
- Excel
- PowerPoint
- OneDrive
- OneNote
- Teams
- Bookings
- Planner
- Shifts
- Viva Engage
- Viva Connections
- Whiteboard
- SharePoint
    - Lists
- PowerPlatform
    - PowerApps
    - PowerAutomate
- Forms
- To Do
- Sway
- Delve

Distansmöten och Audio Video

Produkterna Distansmöten och Audio video omfattar de tjänster och den teknik i form av utrustning (hårdvara) och IT-system (mjukvara) som stöder möten och samarbete. Det finns ofta ett beroende mellan hårdvaran och mjukvara.

Audio och Video (AV)

Inom Audio video , exempelvis:

- Utrustning för mötesrum och konferenser som mikrofoner, skärmar, kameror och högtalare.
- Styrpaneler, dvs tryckkänsliga skärmar genom vilka man styr utrustning och funktioner i en eller flera lokaler.
- Digitala infoskärmar

Distansmöten

Inom området distansmöte hanteras mjukvara som behövs för att ha digitala möten.

De system/plattformar som finns inom produktområdet, är följande:

- Microsoft Teams: Teams har ett överlappande ägarskap och hanteras också inom produktområde Microsoft 365.
- Säkert videomöte (Pexip)
- Cisco CMS
- Cisco VMR (under avveckling, 2023)
- Webex (planerad avveckling kvartal 1 eller 2, 2024)

Roadmap, utvecklingsplan

Områdets utveckling framåt planeras löpande för det kommande året. En översiktlig strategi och utvecklingsplan för produktområdet finns via länk i högerkolumnen.

Förtydligande om digitala vårdmöten

Digitala vårdmöten är ett relaterat område som nyttjar snarlika tjänster men som är utformade specifikt för den nyttjande vårdverksamhetens behov och därmed levereras i form av en verksamhetsspecifik tjänst och ett separat erbjudande. Detta område hanteras inte som del av produkten Distansmöten och Audio Video, utan av ett separat förvaltningsteam med specifikt fokus på hälso- och sjukvård.

Säker dokumentöverföring

Vision

Att genom Säker digital kommunikation (SDK) erbjuda ett tryggt, enkelt och säkert sätt att skicka känslig och sekretessklassad information mellan kommuner, regioner, myndigheter och verksamheter som utför uppdrag åt regionen. Målet är att öka säkerheten och effektiviteten för digital samverkan och informationsutbyte för att på så sätt ge bättre förutsättningar för att ta hand om de individer som behöver stöd.

Att genom Temporär mellanlagring (T:) erbjuda en mapp för att tillfälligt spara ner filer, oavsett filens typ och storlek. Målet är att mappen ska möjliggöra ett mer enhetligt och säkert arbetssätt att hantera information som är tillfällig, känslig eller sekretessbelagd.

Behov

Syftet med Säker digital kommunikation är att kommuner, regioner och myndigheter ska få grundläggande förutsättningar för säkert utbyte av ostrukturerad information mellan varandra. Kanaler som exempelvis fax och brev ska kompletteras och i vissa fall kunna ersättas helt med digital och säker meddelandeöverföring. Plattform och federation tillhandahålls av DIGG.

Temporär mellanlagring (T:) fyller behovet att genom ett enhetligt sätt kunna spara ner information som är tillfällig, känslig eller sekretessbelagd.

Användare

- **Målgrupp SDK**
  Medarbetare med behov av att kunna skicka känslig och sekretessklassad information mellan den offentliga sektorns olika aktörer.

- **Målgrupp Temporär mellanlagring (T:)**
  Medarbetare som har användartjänsten grund eller utökad och använder en VGR PC dator, med behov att mellanlagra filer som är känslig eller sekretessbelagd.

Tjänster

- Säker Digital Kommunikation (SDK)
  - TDialog
  - eDelivery (Domibus)
- Temporär mellanlagring (T:)

Telekom

Produktområde Telekom ansvarar för de regionala verktyg och processer som möjliggör en central hantering av:

- Telefoni - växelsystem och trådlös telefoni
- Telefonist, hänvisning och kontaktcenter
- Larm och meddelandesystem
- Kritisk kommunikation

Telefoni omfattar VGR:s telefonväxel och trådlösa DECT-baserade telefoni för över 55 000 telefonanvändare. Telefonväxeln är ansluten till stödsystem, så som telefonist och hänvisningssystem, kontaktcenter och samtalsbokning.

Larm och meddelandesystem distribuerar ut larm och meddelanden till mobila enheter som till exempel DECT-telefoner, personsökare eller smarta telefoner. VGR:s gemensamma larm och meddelandesystem hanterar över 10 000 akuta larm per år samt ytterligare larm och meddelanden från patienter, medicinska larm, fastighetslarm med mera.

Kritisk kommunikation omfattar bland annat kommunikation via det nationella kommunikationssystemet Rakel och ambulanskommunikation; både kritiska funktioner med krav på hög säkerhet och tillgänglighet under kris eller andra allvarliga situationer.

Livsavgörande kommunikation

Vi ansvarar för att telefonsamtal når rätt mottagare i rätt tid.
Telefonsamtalet är verksamhetens viktigaste kommunikationssätt och kan vara skillnaden mellan liv och död.
Även larm- och meddelandefunktioner är viktiga för våra verksamheter då dessa får personal att agera i allvarliga situationer så som hjärtstopp eller akuta kejsarsnitt. Vi använder också larm och meddelanden för att skapa en tystare arbetsmiljö och snabbare service för medborgare.

Mobilitet

Mobilitet kräver infrastruktur och på VGR har vi många teknologier som används för att kommunicera: DECT, WiFi, 4G/5G, Personsökning via UHF vilka alla har olika egenskaper och är bra på olika saker.

Realtidskommunikation som tal kräver kontinuitet med snabb roaming utan avbrott medan det för en rapporteringsapplikation är viktigare med att snabbt kunna skyffla mycket data men det gör inte så mycket om det blir små korta avbrott. För att få detta att fungera och samtidigt minska på antalet teknologier så krävs en hel del optimering.

Vi strävar också efter att alltid ge verksamheten tillgång till trådburna IP-telefoner tillgängliga för verksamheten. Det för på bästa sätt säkra telefonsamtalet, som kan vara livsviktigt.

Framtidens telefoni

VGR arbetar med att bygga framtidens trådlösa telefoni baserad på mobilt datanät (4G/5G) genom programmet VGR-5G. Målet är att säkerställa täckning inomhus genom egen infrastruktur samt täckning utomhus genom samarbete med externa teleoperatörer.

Det nya mobila datanätet kommer att byggas ut succesivt och allt eftersom ge möjlighet till att helt gå över till mobiltelefoner som arbetsverktyg för telefoni och mobila datatjänster så som larm och meddelanden. Detta skapar också förutsättningar för att använda mobilapplikationer i större utsträckning och därmed också ett mer digitaliserat arbetssätt.

Detta kommer även att möjliggöra och innebära en högre grad av integration mellan traditionell telefonväxel, IP-telefoni och mobiltelefoni.

Telefoni

Produkten Telefoni omfattar de tjänster och den stödjande teknik som krävs för att leverera och hantera telefonväxel och fast telefoni inom VGR.

Telefonväxel

VGR:s telefonväxel är ett IP-baserat system som erbjuder både tal- och videokommunikation, primärt via följande tekniska komponenter:

- **Fast telefon**
  Fysiskt anslutna IP-telefoner anslutna till växeln via IP, vilket ger bäst tillgänglighet och ljudkvalitet.

- **DECT**
  För fast telefoni med mobila enheter använder vi IP DECT där vi har fulltäckning i alla sjukhus på regionen.

- **Cisco Jabber**
  För fast telefoni via en så kallad Softphone; en telefoniapplikation om tillåter att man använder datorn som telefon.

- **MEX**
  Integration av växelanknytningen med mobiltelefon för att kunna ringa och tar emot samtal från växeln via mobilen. Denna förmåga kallas vardagligt för "MEX".

- **Analoga anknytningar**
  För utrustning som kräver traditionella analoga telefonlinjeer (t.ex. FAX) erbjuds adaptrar och konverterare mellan IP-baserad och analog telefoni.

Robust arkitektur och enkel administration

Driftmiljön för växelsystemet är uppbyggd i en redundant och geografiskt distribuerad virtuell servermiljö för att kunna förse verksamheten med telefoni även om det skulle uppstå kommunikationsproblem för specifika dataförbindelser.

Driftmiljön har bland annat följande egenskaper:

- **Klusteruppbyggd i virtuell servermiljö**
  Denna arkitektur ger en mycket hög tillgänglighet.

- **Webbadministration**
  Enkelt åtkomliga gränssnitt för effektiv administration av anknytningar och funktioner.

- **Redundant publik anslutning**
  Sömlösa kopplingar och differentierade anslutningspunkter till multipla teleoperatörer.

- **Standardiserade integrationsgränssnitt**
  Stabil och förvaltningsbara integrationer mot hänvisningssystem, kontaktcentersystem och annan telekomutrustning.

Telefonistarbetsplats, Hänvisning och Kontaktcenter

Produkten Telefonistarbetsplats, Hänvisning och Kontaktcenter omfattar och ansvarar för den teknik och de tjänster som stöttar VGR:s telefonister, hanterar röstbrevlådor, kösystem med återuppringning med mera.

Telefonistarbetsplats och talad hänvisning

Växeltelefonisten är ofta kundens första kontakt med organisationen. Med stöd av IT-verktyget Vision 80/20 kan telefonisten snabbt hjälpa den som ringer in att hitta rätt person, informera om dennes tillgänglighet, samt koppla samtalet vidare. Telefonisterna hjälper också verksamheterna att hänvisa sina telefoner, hantera akuta medicinska larm och se till att dessa når rätt läkare via någon av regionens över 700 jourlinjer.

Telefonisterna besvarar c:a 16 000 samtal per dygn och är placerade i Göteborg, Borås och Trollhättan. Dagtid arbetar ungefär 50 telefonister, nattetid normalt 6.

Talad hänvisning är en funktion för röstbrevlåda som dels informerar om den sökta personens närvaro och tillgänglighet, samt ger möjlighet att lämna ett meddelande i röstbrevlåda.

Inom produkten ingår även ansvar för hantering av VGR:s telefonkatalog på webben.

Kontaktcenter

VGR har c:a 600 telefonköer som medborgare kan ringa till för kontakt med våra olika verksamheter; främst mottagningar inom sjukvården och Folktandvården, men också andra regionala funktioner.

Dessa köer hanteras med stöd av IT-verktyget CC-bridge som tillåter den som ringer att hitta rätt verksamhet via talsvar (så kallad Interactive Voice Response - IVR) eller menyval utan att behöva kopplas vidare manuellt av en växeltelefonist.

Verktyget erbjuder också så kallad "Callback" där den som har blivit placerad i en telefonkö kan välja att ha kvar sin plats i kön men istället bli uppringd när det blivit dennes tur.

Verktyget utgör en kraftfull och flexibel självservicefunktion för den som ringer in. Målet är att erbjuda konsekvent och enkel självservice åt invånare som väljer att kontakt VGR:s verksamheter via telefon.

Samtalsbokning

Samtalsbokning har ca 400 patientingångar för bokning av samtal, där patienten ringer in och får en uppringningstid eller kan lämna ett återbud i en röstbrevlåda främst Närhälsan men även mottagningar på sjukhusen. fördelen för verksamheterna är att det blir tyst miljö och man kan bestämma vilka tider man ringer upp man kan boka samtal hela dagen.

- Boka samtal för att bli uppringd
- Röstbrevlåda
- SMS påminnelser
- Videosamtal
- Videoväxling

Larm och meddelanden

Produkten Larm och meddelanden omfattar den teknik och de stödjande tjänster som krävs för att hantera de c:a 10 000 akuta larm som ställs ut inom VGR varje år.

Våra larm- och meddelandesystem används för att distribuera ut larm och meddelanden till mobila enheter som kan vara DECT telefoner, personsökare eller smartphones, samt nyttjar en redundant driftmiljö för att säkerställa kritisk driftsäkerhet och tillgänglighet.

Systemet hanterar ett antal olika typer av larm och meddelanden:

Akuta Medicinska Larm

Vid akuta medicinska larm (hjärtlarm, traumalarm m.m.) används applikationen Ascom Unite Alarm Agent där larm ställs ut till mobila enheter.

Larm ställs antingen ut via fasta larmknappar eller genom att ringa till telefoniservice som i sin tur ställer ut larmet via en dedicerad applikation.

Alla larm övervakas av telefoniservice (regionens telefonister) som följer upp varje larm och vidtar åtgärder om kvittens från larmmotagaren uteblir.

Det finns även viss integration med fastighetsteknik som möjliggör fysiska åtgärder vid utställt larm; till exempel att hissar körs till rätt våningsplan, att dörrar öppnas och så vidare.

Tyst kallelse (Tyst vårdmiljö)

Tjänsten är en del av VGR:s Ascom-baserade meddelandeplattform som är integrerad mot bland annat trådlöst nätverk (DECT och WIFI) och lokala system för patientkallelse.

Syftet med tjänsten är att:

- Skapa en mer personlig kontakt och snabbare respons till Vårdtagaren genom att kallelser skickas direkt till dedikerad vårdpersonal.
- Skapa en lugnare sjukhusmiljö genom att larmet kommer direkt till en handenhet så att både vårdtagare och vårdpersonal slipper högljudda larmsignaler i korridoren.
- Ge förutsättningar för en mer effektiv fördelning av vårdpersonalens arbete utifrån arbetsbelastning och kompetens.
- Minska stress, ge en bättre arbetsmiljö samt öka fokus hos vårdpersonalen som inte behöver inte höra och ta ställning till alla larm, utan enbart behöver reagera på larm som når den egna handenheten.

Personlarm (Överfallslarm/Bråklarm)

Personlarm konfigureras och distribueras ut till väktare. Hos vissa förvaltningar övervakar personlarm genom en Trygghetscentral.

Larm från medicintekniska produkter

Larm från medicintekniska produkter, exempelvis från patientövervakningssystem, distribueras i meddelandesystemet till mobila enheter. Funktionen är dock ett komplement och kan aldrig ersätta det medicintekniska systemets funktion som primär larmkälla.

Fastighetstekniska larm

Fastighetstekniska larm distribueras ut till drifttekniker. Dessa kan vara hisslarm, brandlarm eller kopplat till funktioner i fastigheten så som ventilation och värme.

Kritisk kommunikation

Produkten Kritisk kommunikation omfattar den teknik och de stödjande tjänster som krävs för att hantera VGR:s säkra och samhällskritiska kommunikationsplattformar Rakel, Säker Digital Kommunikation - SDK, Ambulans kommunikation och Mission Critical PTT.

Dessa kommunikationsplattformar skall inte bara fungera i vardagen, utan har en funktion som är särskilt viktig när situationen är allvarlig och eller under en kritisk situation.

Produkten erbjuder tjänster inom följande områden:

- Radiokommunikation för samhällsviktig verksamhet (Rakel)
- Kritisk kommunikation (MC PTT)
- Säker Digital Kommunikation (SDK)
- Prehospital ärendehantering och kommunikation
- Kommunikationslösningar för Trygghetscentraler och larmcentraler

Rakel

Rakel är Sveriges nationella kommunikationssystem för samverkan och ledning för organisationer med ansvar inom allmän ordning, säkerhet, hälsa och försvar. Rakel är ett robust system med mycket hög tillgänglighet vars infrastruktur ägs av svenska staten.

Inom VGR används Rakel för kritisk kommunikation i vardagen, men också för kriskommunikation vid extra ordinär händelse.

Användare inom VGR är uppkopplade emot Rakelnätet både via trådburna fasta förbindelser samt genom luftburna radioförbindelser.

Inom VGR tillhandahåller vi egna tjänster inom Rakel såsom geografisk positionering av Rakelenheter på en egen digital webbkarta, styrning av portar och förstärkare för inomhustäckning, personsökning med mera. Genom tjänsten Rakel sekretess tillhandahålls även end to end-krypterad kommunikation för våra tjänstepersoner i beredskap dygnet runt, året runt.

Rakel används framför allt inom den prehospitala sjukvården som årligen hanterar c:a 200 000 uppdrag där Rakel är det primära kommunikationssystemet för tal- och data-kommunikation både internt och externt med andra aktörer som polis, räddningstjänst och så vidare.

Kritisk kommunikation

I VGR:s framtida trådlösa 3GPP-baserade infrastruktur kommer en möjlighet finnas som gör det möjligt att på ett säkert och prioriterat sätt kommunicera genom en applikation som vi själva äger och styr över.

Säker digital kommunikation (SDK)

Säker digital kommunikation är en digital infrastruktur som gör det möjligt att på ett säkert sätt utbyta känslig och sekretessklassad information mellan kommuner, regioner, statliga myndigheter och andra offentligt finansierade aktörer.

Kommunikation via SDK sker genom antingen fritext eller PDF-dokument och utgör ett säkert alternativ till fax och vanliga brev.

VGR har en lokal SDK-tjänst ansluten till tjänstens nationella infrastruktur som i sin tur förvaltas och levereras av Inera AB.

Digitala plattformar

Produktområde Digitala Plattformar ansvarar för drift, förvaltning och vidareutveckling av grundläggande infrastrukturella plattformar för utveckling och leverans av IT-stöd i form av tjänster för container- och serverhosting, datalagring, integration med mera.

De tjänster som erbjuds är återanvändbara, skalbara samt har en hög säkerhets- och tillgänglighetsnivå.

Plattformstjänsterna tillhandahåller en stabil men ändå flexibel driftmiljö och ger därmed förutsättningar för andra team att i sin tur leverera stabila och säkra IT-stöd samtidigt som de stöttar innovation, modernisering och digitaliseringsarbete inom regionen.

Förmågor

Produktområdet levererar mot dessa övergripande förmågor:

- Leverera paketerade hostingtjänster
- Leverera containerplattform
- Leverera lagringstjänster och dataskydd
- Leverera infrastruktur för virtualisering
- Leverera övervakningsplattform
- Leverera plattform för DevOps-verktyg
- Leverera plattform för integrationer
- Leverera plattform för datahantering
- Leverera plattform för AI
- Leverera plattform för databas

Principer

- Allt ska levereras via självservice
- Allt som kan automatiseras, ska automatiseras
- Vi behandlar våra plattformar som produkter (Platform-as-a-product)
- Tjänsterna är väldefinierad och flexibla för att möte våra kunders behov på bästa sätt.
- Tjänsterna och komponenterna är alltid valfria att använda men det ska inte finnas någon tvekan.

AI-plattform

Produkten AI-plattform innefattar tjänster och stödjande teknik som krävs för att hantera utveckling och träning av AI/ML-modeller. Plattformen

skapar förutsättningar för våra olika verksamheter att jobba med prediktion och automation och bedriva forskning.

Distribution och access till plattformen sker via containerteknik där användaren upprättar sina utvecklingsmiljöer på plattformens infrastruktur.

AI-plattformen är inte begränsad till en viss typ av utvecklingsmiljö och har också stöd för flera olika programvarubibliotek inom AI/ML-området.

Förmågor

- Beräkningskraft (GPU & CPU)
- Snabb datalagring (för ML-träning)
- Kapacitetshantering (orkestrerar och schemalägger jobben)

Databasplattform

Produkten Dataplattform omfattar de tjänster och den stödjande teknik som hanterar och möjliggör insamling, bearbetning, analys, presentation och tillgång till betrodd data i ett brett och distribuerat applikationslandskap, för både operativa och analytiska applikationer.

De tjänster som erbjuds stöds av teknik och kapacitet från både interna och externa driftsmiljöer.

Förmågor

Det viktigaste tekniska förmågor som erbjuds eller kommer att erbjudas inom produkten är:

- Datalagring
- Dataåtkomst
- Datavirtualisering
- Data management
- Operational Data Lake
- Datapipelines
- Analysplattform
- Datakvalitet
- Databaslösning
- Data Movement
- Automatiska datahanteringsprocesser
- Datareplikering
- Data stream
- Datatransformation ETL
- Datahistorik

- Rapporetering
- Datasäkerhet
- Managed databas
- Datakatalog

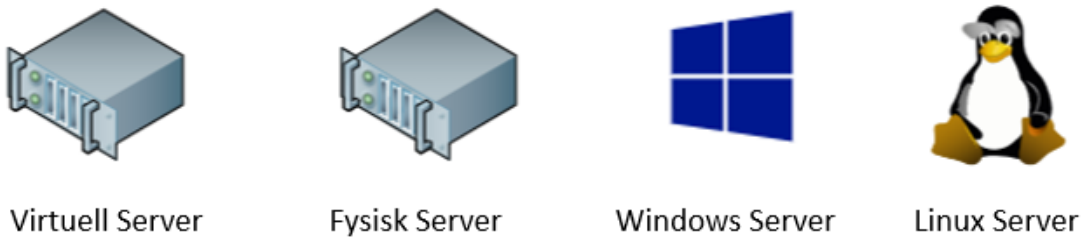
Tekniska komponenter

Ovanstående tekniska förmågor realiseras i huvudsak genom följande tekniska komponenter:

- SQL-databas (MS SQL Server, Oracle, MySQL med flera)
- NoSQL-databas (Mongo, Redis, med flera)
- Datavirtualisering (Denodo)
- SQL Server Integration Services
- SQL Server Reporting Services
- SQL Server Analysis Services
- SQL Server Big Data Clusters
- PowerBI med Data Gateway
- Datakatalog (Ab intio)
- Automatiska datahanteringsprocesser (Ab intio)

Hosting

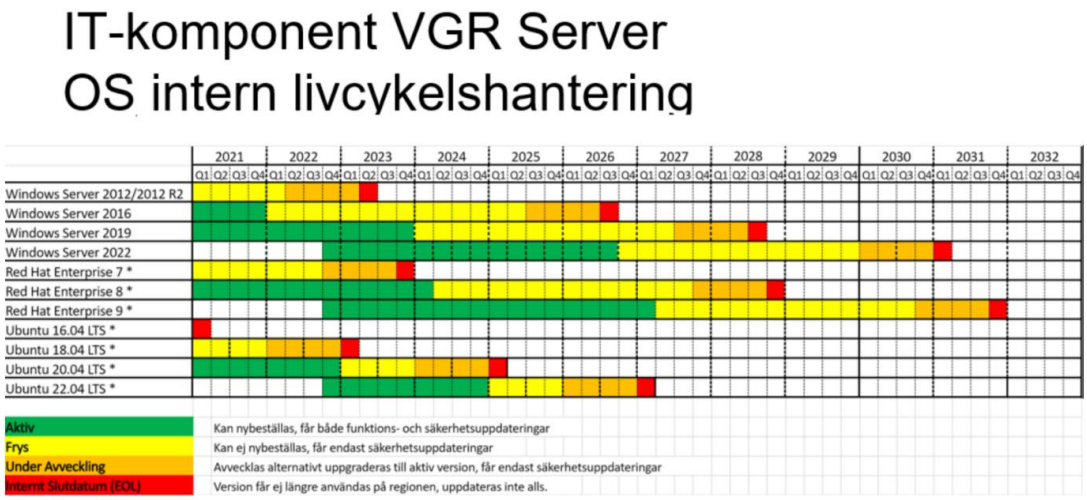
Produkten Hostingplattform tillhandahåller och livscykelhanterar hostingtjänster där ett antal serveroperativ är vår första tjänst. De Server OS vi levererar som tjänst baseras på Windows Server, Ubuntu och Red Hat Linux Server.



VGR kan tillhandahålla servertjänster i form av fysiska och virtuella servrar i en mängd olika konfigurationer. Virtuella servrar är standard. Fysiska servrar används enbart vid särskilda behov och efter prövning. I standardtjänsten ingår serverbackup (3 månader lagring), övervakning av grundfunktionalitet, standardiserad patch-hantering av operativsystem och antivirus som en del av tjänsten. Förändring (ökning/minskning) av server resurser beställs separat genom ärende i ITSM-verktyg.

Samtliga operativsystem som supporteras av VGR har en intern livscykel som följer underliggande mjukvaruleverantörs livscykel. Servrar som driftas på plattformen måste följa dessa livscykelplaner för att VGR skall kunna ta ansvar för drift av dessa.

För mer information om gällande livcykelplan för VGR, se nedan bild. I den kan man utläsa vilka versioner av olika OS som är aktiva, frysta, under avveckling samt vilket VGR-internt slutdatum som är satt (EOL, End Of Life).



Leverantörer tilldelas inte access via Root konto eller Windowskonto med RID 500 utan använder personliga konton i VGRs befintliga inloggningstjänst, och servrar får endast fjärrstyras via VGRnet eller via av regionen godkänd uppkoppling. Installation av programvara sker av VGR eller gemensamt med leverantör. Servern placeras i VGR:s Datacenter.

Samtliga teknikområden rörande drift och serverrelaterade tjänster kan baseras på 24/7 tillgänglighet om så erfordras. Tillgänglighet ska dock vara i nivå med verksamheternas behov för att undvika onödigt resursutnyttjande.

Servrar är normalt sett tillgängliga 24/7. Dock skiljer supportnivåerna beroende på verksamhetens krav. VGR utför förebyggande underhållsarbete såsom patchning i förutbestämda servicefönster.

VGR erbjuder en teknisk plattform som (gäller både fysisk och virtuell):

- Är centralt hanterad och har en standardiserad teknisk serverplattform som är flexibel, skalbar och tillgänglig.
- Har servrar som är integrerade med regionens centrala katalogtjänst.
- Är en standardiserad serverplattform baserad på modern teknik där outnyttjad kapacitet återanvänds.

DevHub

Kubernetes

Vår vision är att vi ska tillhandahålla en fullfjädrad container miljö samt stöttande verktyg som är fullständigt automatiserad, definerad som kod och konsumeras endast via self-service.

Produkten omfattar tjänster och stödjande teknik för orkestrering och hantering av containeriserade applikationer och dess resurser på med stöd av containerplattformen Kubernetes.

Vi tillhandahåller också tjänster och den stödjande teknik som möjliggör för applikations- och integrationsutvecklare att källkodshantera, produktionsätta, hantera drift och övervaka applikationer på ett automatiserat och säkert sätt.

Kubernetes fungerar som en orkestreringsmotor som gör det möjligt att enkelt skala, hantera och övervaka applikationer med sina komponenter på en distribuerad infrastruktur. Plattformen levereras i dagsläget från ett datacenter, i Skövde.

Vid leverans av en applikation till ett Kubernetes-kluster bygger man vanligtvis en container-bild som innehåller applikationen. Därefter distribueras den till klustret för att exekveras på Kubernetes-noder.

Med stöd av Kubernetes kan man bland annat:

- Automatisera distributionen av sina applikationer. På detta sätt säkerställs att de är tillgängliga och skalbara i olika miljöer; som utveckling, test och produktion.
  Detta ökar driftsäkerheten och minskar risken för driftstopp
- Skala de containeriserade applikationerna på ett flexibelt och säkert sätt
- Hantera resurser som processorer, minne och lagring för applikationer
- Enkelt distribuera applikationer över flera instanser eller noder. Kubernetes har ett inbyggt stöd för avancerad dirigering av trafik och lastdelning

För mer information om Kubernetes läs här; https://kubernetes.io/

Kubernetes tjänstepaket

Vi erbjuder ett tjänstepaket till de kluster vi levererar där det finns möjlighet att välja bort hela eller delar av tjänstepaketet. Komponenterna i det grundläggande paketet består av ett flertal öppna källkodsprojekt från Cloud Native Compute Foundation (CNCF) ekosystem.

Dessa komponenter inkluderar följande:

Argo CD

Ett verktyg för att hantera och implementera Kubernetes-applikationer samt infrastruktur som kod. Argo CD möjliggör automatisk tillståndshantering och synkronisering av applikationer i ett Kubernetes kluster med konfigurationsfiler. Konfigurationsfilerna finns lagrade i ett versionshanteringssystem, till exempel Git.

- Ger möjlighet att definiera ett önskat tillstånd, till exempel applikationskonfiguration, för att automatiskt synkronisera klustret med önskat tillstånd. Vilket innebär att om man ändrat en applikation i Git-kodförråd kommer Argo CD att upptäcka ändringen och automatiskt synkronisera klustret med den nya konfigurationen
- Med Argo CD kan man validera applikationskonfiguration, övervaka applikationstillstånd, hantera driftsättningar och återladdningar
- Stödjer olika autentiserings- och auktorisationsmetoder för att hantera åtkomstkontroll

För mer information om Argo CD, läs här: https://github.com/argoproj/argo-cd

Ingress

Ingress är en resurs som används för att hantera inkommande nätverkstrafik till applikationer i ett Kubernetes-kluster. Ingressresursen fungerar som en extern ingångspunkt till Kubernetes-klustret, där inkommande nätverkstrafik kan riktas till rätt Kubernetes-tjänst för hantering.

- Ingress-resursen definierar en uppsättning regler för att styra inkommande trafik baserat på HTTP/HTTPS URI-rutter eller domännamn till rätt Kubernetes-tjänst. Detta gör det möjligt att hantera flera virtuella värdar och hantera URL-sökvägar för inkommande anslutningar
- Vi använder oss av Nginx ingresshanterare

För mer information om Nginx Ingress, läs här: https://kubernetes.github.io/ingress-nginx/

Prometheus

Prometheus är en systemövervakningslösning som används för att samla in och lagra metriska data från olika källor med möjlighet att visa och utforska denna data i realtid. Prometheus består av flera komponenter, inklusive en tidsseriedatabas som samlar in data från applikationer och infrastrukturkomponenter.

Med Prometheus

- Kan man övervaka prestanda och status för applikationer och infrastruktur i realtid, identifiera problem och felsöka problem snabbt.
- Få ett webbgränssnitt som gör att man kan visualisera och analysera data.

För mer information om Prometheus, läs här: https://github.com/prometheus/prometheus

Loki

Loki är en logghanteringslösning som är utformad för att hantera och analysera loggdata. Den data som genereras av applikationer och infrastruktur i tex Kubernetes-kluster. Loki består av flera komponenter:

- Loggbearbetningsmotor
- Indexmotor
- Gränssnittswebbapplikation

Dessa komponenter arbetar tillsammans för att samla in, bearbeta, lagra och fråga efter loggdata.

För mer information om Loki, läs här: https://github.com/grafana/loki

Grafana

Grafana är en plattform för dataanalys och visualisering som används för att övervaka och analysera prestanda och status för applikationer och infrastruktur. Det är en webbapplikation som kan integreras med olika databaser och datakällor, inklusive tidsseriedatabaser som Prometheus.

Med Grafana

- Kan man skapa anpassade och interaktiva informationspaneler som visualiserar data på ett lättförståeligt sätt, vilket gör det enklare att förstå och analysera data och identifiera problem och förbättringsområden.
- Får man en mängd inbyggda verktyg för att utföra dataanalys, inklusive aggregationsfunktioner, filtreringar och diagramtyper.

För mer information om Grafana, läs
här: https://github.com/grafana/grafana

Containerregister

Vi erbjuder också containerregister genom Harbor. Registret används för att hantera, lagra och distribuera containrar på ett enkelt och säkert sätt. Med Harbor lagras containrar lokalt i VGR:s miljö vilket gör att de inte behöver hämtas från ett externt register varje gång de behövs.

Containrarna i registret undersöks regelbundet för att hitta eventuella sårbarheter vilket medför en hög säkerhet.

För mer information om Harbor, läs här: https://goharbor.io/

Källkodshantering och DevOps

Gitlab är en webb-baserad git repository och devops verktyg som möjligör utveckling och driftsättning av applikationer.

Köhantering

Active MQ är en distribuerad köhanteringstjänst som möjliggör asykron kommunikation mellan olika applikationer.

Idag används Active MQ övervägande av interna komponenter på plattformen men vårt mål är att kunna erbjuda denna tjänsten även externt så att applikationsutvecklare behöver inte drifta egna meddelandetjänster.

Static application security testing

SonarQube är en öppen källkodsplattform utvecklad av SonarSource för kontinuerlig inspektion av kodkvalitet för att utföra automatiska granskningar med statisk analys av kod för att upptäcka buggar, bristfallig kod och säkerhetsbrister i flera programmeringsspråk, såsom Java, .Net m.m.

Logganalys

ELK-stacken är en stack som består av tre populära projekt: Elasticsearch, Logstash och Kibana. Den ger möjligheten att samla loggar från alla våra system och applikationer, analysera dessa loggar och skapa visualiseringar för applikations- och infrastrukturövervakning, snabbare felsökning, säkerhetsanalys och mer.

API Gateway

Mulesofts API gateway Anypoint erbjuder en helhetsperspektiv kring API:er, från API-first utveckling till drift och övervakning. Denna tjänsten används primärt av ICC än så länge men vi vill erbjuda tjänsten till alla utvecklare för att kunna bygga upp en nätverk av API:er som kan återanvändas inom VGR.

Lagringstjänster och dataskydd

Produkten lagringstjänster och dataskydd möjliggör användandet av säkra lagringsytor med hög tillgänglighet, skalbara och geografiskt skyddade.

Detta åstadkommer vi med tekniker såsom snapshot, replikering, erasure coding, raid och backup. För åtkomst till ytorna för system, applikationer, datorer eller servrar så stöder vi SMB, NFS, S3 samt blocklagring (SAN).

Beställning

Lagringstjänster erbjuds och beställs via självbetjäning genom den tekniska katalogen i VGR:s interna ITSM-verktyg Plexus eller med stöd av tekniker genom att initiera ett ärende.

Leverantörer

Vi använder lösningar från IBM, NetApp, DELL och Hitachi.

Säkerhet och skalbarhet

Säkerhet uppnås med hjälp utav olika tekniker för dataskydd tillsammans med antivirus och ransomware-skydd.

Skalbarhet uppnås genom att vi använder Enterprise-system med funktioner för hög tillgänglighet som är geografiskt distribuerade mellan 2-4 separata datacenter.

Våra utdelade lagringsytor kan skalas från ett fåtal gigabyte upp till flera petabyte.

Virtuell infrastruktur som tjänst

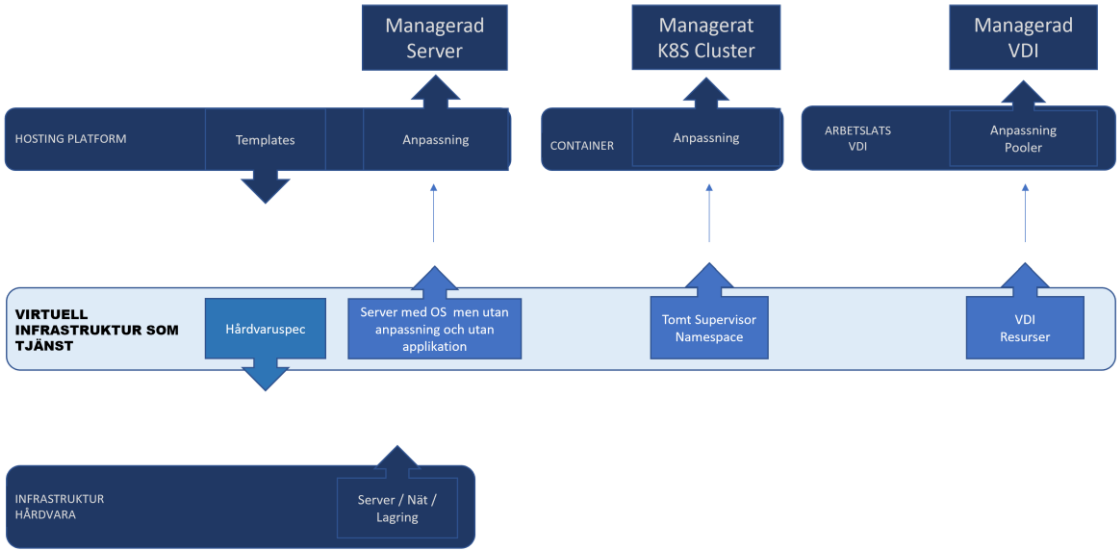
Genom att låta en fysisk server köra flera operativsystem samtidigt kan serverkraft fördelas mer optimalt med effekten att redundans och tillgänglighet ökar.

Modern hårdvara är så pass kraftfull att det är möjligt att installera många servrar eller klienter på en och samma fysiska maskin. Med hjälp av mjukvara kan de enskilda virtuella maskinerna dessutom transparent förflyttas från en fysiska server till en annan under pågående drift.

Produkten Virtuell infrastruktur omfattar leverans av virtuell kapacitet i form av CPU, minne, lagring och nät till virtuella maskiner (VMs) med OS, namespaces för Kubernetes K8s samt VM Services.

Produktteamet ansvarar för att:

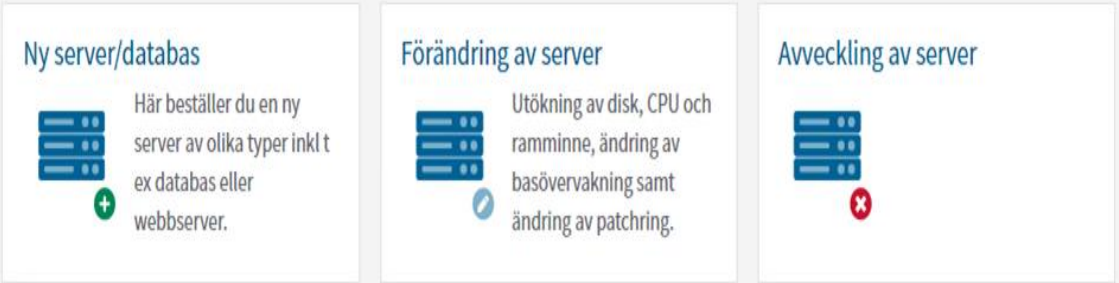
- Ställa krav på och konsumera fysisk kapacitet i form av hårdvara, datalagring och nät.
- Etablera en intern molnlösning för leverans av kapacitet med tillhörande självservice, automatisering, drift, säkerhet, analysmöjligheter och livscykelhantering.
- Leverera traditionella virtuella maskiner (VMs) som stöd åt produkterna Hostingplattform och VDI (under produktområde Arbetsplats), moderna driftmiljöer för Kubernetes samt erbjuda möjligheten att komplettera dessa med GPUs för AI och grafiktillämpningar.
- Säkerställa prestanda, tillgänglighet och motståndskraft mot störningar hos levererade tjänster.



Förmågor

De förmågor som erbjuds inom produkten beställs direkt via självservice av respektive konsument, och inkluderar:

- Beställning, förändring och avvecking av VMs (främst för produkt Hostingplattform)
- Skapa resurser för hantering av pooler (främst för produkt VDI)
- Skapa namespace (främst för produkt Kubernetes)
- Generell virtuell kapacitet i form av minne, cpu, disk och nät, med hantering och säkerhet
- Uppföljning av prestanda på och nyttjande av levererade tjänster



Primära konsumenter

Vi levererar i första hand tjänster som stöttar produkterna Hosting Plattform, Kubernetes och VDI som stöd åt sina respektive förmågor och erbjudanden.

Kunskap

Vi är med och stöttar vid frågor runt miljön och vad den erbjuder rent praktiskt i form av prestanda, konfigurering, dimensionering, automatisering, självservice osv.

Bra att tänka på vid design eller kravställning

- K.I.S.S - "Keep it Simple" - är alltid att föredra framför komplexitet.
- Beställ enligt standardval och undvik anpassade lösningar i möjligaste mån.
- Beställ vad som behövs i närtid för att sedan över tid komplettera med prestanda och utrymme. VGR styr behoven av kapacitet och prestandatilldelning.

Bra att veta om driftsmiljön

- I dagsläget använder VGR vCenter 7 och ESXi 7 för sin virtuella leverans. Version 8 är under tester och planeras införas så snart testerna är klara. Framtida uppdateringar införs sedan löpande.
- En virtuell maskin tilldelas inte mer resurser än den anses behöva.
- Vi överallokerar aldrig den fysiska hostens minne (vMEM).
- Vi överallokerar cpu (vCPU) men undviker köer, dvs prestandapåverkan.
- Större diskar inne i OS (> 2TB) delas ute i miljön upp i flera mindre (<2TB) och kopplas sedan logisk ihop igen till en större inne i OS (ex med dynamiska diskar), alternativ (hellre) kan NAS-utrymme kopplas på inne i OS för att leverera större utrymme.
- Plattformen uppdateras kontinuerligt för säkerhet och funktion.
- Firmware för hårdvaror hanteras kontinuerligt för ökad säkerhet och funktionalitet.

- HA är aktiverat i klustren – för hantering av hårdvarufel.
- Klustren skapas alltid med kapacitet för att hantera minst ett hårdvarufel.
- VMotion är aktiverat i klustren – för prestanda och planerat underhåll dagtid.
- DRS är aktiverat i klustren – för prestanda och placeringsregler.
- VMware Fault Tolerant används inte.
- VMware DPM används inte för att stänga ned hårdvaror (de är alltid på).
- Storage VMotion är aktiverat i klustren – för utrymme enbart.
- Säkerhetskopiering sker på Image nivå och möjliggör återläsning ned till filnivå.
- Enbart behörig personal inom VGR har åtkomst till vCenter.
- Snapshots används enbart vid backuptagande och då normalt enbart nattetid och vid låg belastning.
- Ström/prestanda i hårdvara är konfigurerad enligt ’OS Control’ och ’High performance’.

Digital infrastruktur

Digital Infrastruktur

Vi arbetar aktivt med att utveckla och bygga en robust infrastruktur som möjliggör tillförlitliga och snabba digitala tjänster. Med genomtänkta leveransprocesser och effektiv livscykelhantering säkerställer vi att våra tjänster inte bara är tillgängliga, utan också optimerade för hög prestanda och säkerhet.

Leverans och livscykelhantering

Vår leverans skall vara utformad för att snabbt och säkert rulla ut tjänster som är vitala för våra konsumenter. Genom hela livscykeln, från planering och implementering till underhåll och uppdatering, är vi noggranna med att vi uppfyller framtagna kvalitets- och säkerhetsstandarder. Vårt mål är att våra tjänster ska vara tillförlitliga och hållbara, vilket innebär att de ska kunna anpassas efter förändrade förhållanden och krav.

Operativt Center

Vårt operativa center är viktig i vår övervakningsstrategi, med personal på plats 24/7 för att säkerställa att våra system alltid är online och fungerar som de ska. Teamet agerar snabbt på incidenter, vilket minimerar störningar och förebygger en oavbruten verksamhet.

Säkerhetsfokus

Robusthet och säkerhet är centralt i allt vi gör. Vi lägger mycket energi i att säkerställa att vår infrastruktur har bästa motståndskraft mot både interna och externa hot och att våra säkerhetsåtgärder skyddar både data och system. Med godkända säkerhetsprotokoll och -kontroller strävar vi efter att hålla våra användare och deras information säkra.

Automatisering och användarcentrerade tjänster

Automatisering är en nyckel till att erbjuda högkvalitativa och användarvänliga tjänster. Genom att hela tiden se över behovet av manuella processer och förenkla komplexa system erbjuder vi våra användare smidiga tjänster som tillgodoser behov. Genom att tillhandahålla lösningar som är enkla att beställa och använda, och ständigt förbättra genom användarfeedback når vi våra mål.

Framåtblick

Vi kommer att fortsätta att stärka vår infrastruktur - säkerhet, tillgänglighet och robusthet - samtidigt som vi ständigt förfinar våra tjänster för att vara mer användarvänliga och automatiserade. Genom nära samarbete med våra konsumenter och ha djup förståelse för våra deras behov, levererar vi en tjänst som inte bara uppfyller, utan överträffar förväntningarna.

Applikationspublicering

Produkten Applikationspublicering omfattar de tjänster och den stödjande teknik som tillgängliggör och publicerar applikationer på ett säkert, snabbt och enkelt sätt.

Produkten har förmågan att agera grindvakt för bakomliggande infrastruktur samt möjliggöra åtkomst till känsliga resurser baserat på t ex identitet, geografi/lokation, status etc.

Produkten ska leverera robusta tjänster med fokus på säkerhet, tillgänglighet och användarupplevelse. Produkten erbjuder fördefinierade publiceringsytor för applikationer och tjänster mot internet, Sjunet och VGR:s interna driftsnät VGRnet.

Produkten kallas ibland även ADC-plattformen och hanteras av ADC-Teamet.

ADC (Application Delivery Controller) är ett generellt begrepp för denna typ av produkt.

ADC är en utveckling av den traditionella lastbalanseraren och är idag en kombination av reverse proxy, vpn gateway, brandvägg och dns

Vision och målbild

- En konsoliderad publiceringsyta för applikationsaccess
- Skapa hög lägstanivå
- Förhindra att okrypterad, osäker och gammal teknik blir tillgänglig mot konsumenter/klienter
- Isolera äldre och osäkra applikationer
- Grindvakt för datacenter, förhindra direktaccess från klienter

En standardisering gällande plattformar. Ökat skydd för interna och externa applikationsleveranser

Förmågor och Funktioner

Tillgänglighet

Exponerade tjänster skall alltid vara nåbara och med god prestanda. Detta åstadkoms genom:

- Lastbalansering, fördela belastning mot bakomliggande servrar
- Hälsokontroller
- SSL/TLS-terminering
- Optimering
- Geo-lastbalansering

Åtkomstkontroll

Stoppa irrelevant och icke önskvärd trafik på så tidigt stadie som möjligt.

- Pre-Auth med Federation
- Single Sign-on
- mTLS

Säkerhet

Produkten kan addera ett antal säkerhetsfunktioner på de applikationer/tjänster som publiceras där vissa är valbara och andra obligatoriska.

Obligatoriska säkerhetsfunktioner

- **Cipher Suites**
  Fördefinierad konfiguration baserad på OWASP-rekommendationer för att säkra en hög lägsta nivå när det kommer till ciphers och kryptering, t ex minst TLS 1.2 och uppåt, Här kan vi t ex skydda

tjänster med äldre implementationer av SSL och samtidigt förenkla administration av certifikat.

- **WAF - Web Application Firewall**
  En baseline-konfiguration adderas till alla applikationer och tjänster vilket ger möjlighet att fånga vanligt förekommande attacksignaturer, typ cross site scripting, SQL injections etc.

- **IP Intelligence**
  Filtrera bort skadliga avsändare, baserat på geografi eller ryktesdatabas från Brighcloud

Valbara säkerhetsfunktioner:

- **FW (firewall)**
  Traditionell brandväggsfunktionalitet, dvs source och destinations IP och portar.

- **Geo-FW (location-based firewall)**
  Filtrera trafik baserat på geografi

Datacenter Nätverk

Produkten Datacenter nätverk omfattar de tjänster och den stödjande teknik som möjliggör att all nätverkstrafik inuti VGR Datacenter, Extern-block och management-block kan transporteras på ett snabbt och säkert sätt. För att åstadkomma detta använder vi oss av ett antal olika tekniker och produkter som vi har till vårt förfogande.

Extern block

Lokalt nätverk för alla externa förbindelser och perimeter brandväggar.

Management block

Lokalt nätverk för all kärnutrustning som behöver fjärrmanageras.

Brandväggar

Vi använder brandväggar till många saker inom vårt nätverk. Det främsta användningsområdet är att skydda access till eller ifrån applikationer och system med regelverk. De används även för att identifiera användare, applikationer och system samt att blockera virus, malware och kommunikation till kända dåliga ip adresser.

Switchar

Switcharna är inkopplingspunkt för all hårdvara i våra Datacenter, extern block och management block. Datan inuti dessa miljöer transporteras

snabbt och säkert med ett konsekvent trafikmönster, vare sig det är nord/syd eller öst/väst.

IT-Utrymme

It-utrymme

Våra it-utrymmen inom Västra Götalandsregionen är en grundläggande del av it-infrastrukturen som stödjer en mängd olika funktioner och tjänster. Dessa it-utrymmen är kravställda och utformade för att vara tillgängliga, säkra, effektiva och skalbara, vilket möjliggör en anpassningsbar och robust it-miljö.

Datahall

En datahall är ett utrymme avsett för att rymma servrar, datalagringsutrustning och andra stora it-system. Detta utrymme är designat för att hantera stora mängder data, med fokus på hög driftsäkerhet, effektiv kylning och energihantering, samt säkerhet mot fysiska hot.

Teknikrum

Med teknikrum avses ett it-utrymme som förvarar en mindre mängd it-utrustning. Lokalen bör vara anpassad för it-drift, men är inte uttalat avsedd eller projekterad för det ändamålet.

Infrastruktursrum

Infrastruktursrum är centralt för regionens nätverks- och kommunikationsinfrastruktur. Det innehåller nätverksenheter som switchar och routrar och är avgörande för att säkerställa stabil och säker dataöverföring inom regionen.

Zonrum

Ett zonrum används för att skapa säkerhetszoner inom it-infrastrukturen. Det agerar som en spridning- eller övergångszon mellan olika nivåer i nätverket.

Korskopplingsrum
Korskopplingsrummet är en centralpunkt för nätverkskoppling och distribution. Härifrån styrs och hanteras fysiska kopplingar mellan olika nätverkssegment och enheter. Dessa rum är avgörande för att underlätta effektiv nätverkskommunikation och möjliggör flexibel anpassning av nätverksstruktur vid behov.

Konnektivitet

Produkten Konnektivitet omfattar nätverksinfrastrukturen i VGR och den teknik som behövs för att kunna tillhandhålla datakommunikation till användaren.

WAN (wide area network)

Innehåller flertal routrar som möjliggör datakommunikation mellan olika geografiska områden inom VGR. En router är en nätverksutrustning som kopplar samman fler olika nätverk. Routrar skickar datapaket till olika nätverk. Data som skickas kan till exempel vara en webbsida, e-post eller vårdapplikationer.

LAN (local area network)

Innehåller flertal switchar som möjliggör lokal datakommunikation i ett begränsat geografiskt område inom VGR. Det kan tillexempel vara nätverket för ett sjukhus eller vårdcentral. En switch är en nätverksutrustning som ansluter enheter till det lokala nätverket. Det kan bland annat vara datorer, skrivare, ip telefoner och mt utrustning.

Nätverksförbindelser

Nätverksförbindelser gör det möjligt att koppla samman routrar och switchar mellan olika geografiska områden som tillexempel mellan sjukhus och vårdcentraler. Det omfattar även förbindelser till externa nätverk som internet, sjunet och SGSI. Det finns olika typer av nätverksförbindelser med olika användningsområden. Vanligaste typen i VGR är tjänsteförbindelser där en leverantör skapar en förbindelse via deras infrastruktur. En annan typ är svartfiber där VGR hyr fiber av en leverantör för att bygga en egen förbindelse.

Mobil konnektivitet

Produkten Mobil Konnektivitet omfattar den trådlösa nätverksinfrastruktur och övrig teknik som behövs för att tillhandhålla användare med trådlös datakommunikation inom VGR.

WiFi

Består av accesspunkter som agerar radiosändare samt central utrustning så som Wireless Controllers som tillsammans tillhandahåller trådlös uppkoppling för datakommunikation.

Tjänster som levereras är bland annat trådlösa nätverket VGR samt det publika gästnätverket VGR Publikt.

Miljön består av cirka 12 500 trådlösa accesspunkter för att täcka utpekade ytor där behov har identifierats. VGR Wifi är inte heltäckande, det är därför viktigt att säkerställa att Wifi-täckning finns innan en tillämpning som ska nyttja Wifi tas i bruk. Om Wifi-täckning saknas behöver detta beställas.

VGR Wifi levereras på frekvensbanden 2,4GHz samt 5GHz med 802.11ac eller senare. På grund av dom tekniska begränsningar som finns inom 2,4GHz-bandet (Lite tillgänglig frekvens samt mycket störningar från andra Wifi-nät och annan icke-Wifiutrustning) rekommenderas enheter att primärt koppla upp sig mot 5GHz. Enheter bör också stödja Wifi 6E för att stödja nya tillgängliggjorda frekvenser på 6GHz-bandet.

SSID VGR är det nätverksnamn som leder till produktionsnätet. Detta nät stödjer trafikprioritering (QoS) där infrastrukturen litar på prioriteringsmarkeringar som handenheten gör.

För att kunna koppla upp sig mot SSID VGR behöver handenheten stödja dom autentiseringsmetoder som används. Det innebär att enheten behöver ha ett korrekt enhetscertifikat genererat från VGR PKI-miljö, enheten behöver också ha en WPA-supplicant som stödjer WPA3 och kan autentisera med WPA2/3 Enterprise med EAP-TLS.

Bakom SSID VGR finns ett klientsegment där handenheten tilldelas en IP med DHCP. Om informationsägaren och/eller applikationsägaren bedömer att en enhet ska segmenteras sköts detta med standardiserad nätsegmentering (VLAN och olika nätsegment, VRF-teknik samt Brandväggar). Vid autentisering kan en handenhet placeras i önskat nätsegment baserat på dess identitet.

All trafik som genereras på VGRs trådlösa nätverk tunnlas tillbaka till centrala punkter inom VGRnet (Göteborg, Borås, Skövde, Trollhättan). Dessa centrala punkter har redundant infrastruktur för att hantera plötsliga fel.

I Produkten ingår också system för att konfigurera, hantera, dokumentera samt övervaka accesspunkter.

Mobilnät

Möjliggör mobil uppkoppling via 3GPP standarder tex LTE och/eller 5G-nätverk.
Denna nya teknik är för tillfället i stadie Labb/Pilot.

- **Radionät**
  Trådlöst accessnät som möjliggör kommunikation mellan slutanvändarenhet och kärnnät.

- **Kärnnät**
  Komponenter mellan accessnätet och andra nätverk, till exempel VGRnet. Inkluderar ett antal komponenter som möjliggör funktionalitet i mobilnätet för slutanvändare samt sköter funktioner såsom autentisering och trafikprioritering.

Nätverksservice

Produkten Nätverksservice omfattar de tjänster och den stödjande teknik som behövs för att knyta samman VGR:s nätinfrastruktur för att skapa ett användarvänligt, flexibelt och förvaltningsbart nätverk.

Produkten består av tre subfunktioner med olika förmågor:

DDI

DDI (DNS, DHCP & IPAM) inkluderar de grundläggande komponenter som möjliggör adressering och förvaltning av den regionala nätinfrastrukturen. Dessa inkluderar:

- **DNS - Domain Name System**
  Gör det möjligt att slå upp en adress, till exempel vgregion.se till en adress som en dator kan förstå. Bryggar gapet mellan en dator och vad som är mänskligt läsligt.

  Vi hanterar även alla andra domäner som är kopplade till verksamheter inom Västra Götalandsregionen, och hanterar domänregistreringar och förnyelser av nya och gamla domäner via upphandlade avtal.

- **DHCP: Dynamic Host Configuration Protocol**
  Ger möjlighet för att en godkänd dator eller enhet ska kunna automatiskt konfigureras med alla inställningen den behöver för att fungera på nätverket direkt när enheten startar eller när en nätverkslänk etableras.

- **IPAM: IP Address Management**

Planerar alla IP Adress utrymmen i regionen för att hantera nuvarande och framtida behov.

All DDI hos VGR hanteras i våran Infoblox-plattform för att skapa en central plats för all hantering och konfigurering.

Målbilden för DDI är att ha en så effektiv, redundant och robust miljö som möjligt för att se till så att verksamheter kan fortsätta sitt arbete även i katastroftillstånd, samtidigt som den kan konsumeras så flexibelt som möjligt under vanlig drift.

Nätverkstid

Funktionen nätverkstid säkerställer tillgång till gemensam och synkroniserad tidsangivelse och är en vital del för att se till så att nätverksanslutna system runt om i Västra Götalandsregionen fungerar på ett optimalt och säkert sätt. Funktionen erbjuds via följande komponent:

- **NTP: Network Time Protocol**
  Möjliggör synkronisering av tidsangivelse med hög noggrannhet i nätverksanslutna enheter och system med stöd av tidsservrar som i sin tur är anslutna till atomur, GPS och andra former av radiobaserade klockor.

  Nätverksservice ansvarar för att den centrala funktionen har en hög tillgänglighet och optimal funktion.

Net Management

Denna funktion är en del av den övergripande förmågan till effektiv leverans inom produktområde Digital Infrastruktur som helhet.

Målbilden är att Nätverksservice ska kunna bistå med miljöer, plattformar, ramverk och kompetens kring utveckling och automation av nätverkstjänster, som i sin tur kan nyttjas av andra produkter inom Digital Infrastruktur i syfte att göra områdets gemensamma leverans så effektiv som möjligt.

De delförmågor som erbjuds inom produkten Nätverkstjänster inkluderar:

- **Nätverk och Plattformsmanagering**
  Inom denna förmåga erbjuds plattformar som ska ge möjlighet till central hantering av nätverksenheter, effektivt hantera omfattande förändringar, få en överblick och helhetsbild av status i nätverket med mera. Sammanfattat en “Single point of Configuration & Administration".

  Nätverkstjänster har även möjlighet att hjälpa till med utvärdering och managering av relaterade plattformar som övervägs eller implementeras inom Produktområdet.

- **Stödtjänster**
  Interna verktyg och stödtjänster för att kunna validera, övervaka och i slutänden leverera så optimal infrastruktur som möjligt såsom interna speed-test tjänster för att kunna mäta våra länkar, lagring för nät-infrastruktur med mera.

- **Stöd vid utveckling**
  Nätverksservice utvecklar arbetssätt, kod och verktyg för att kunna effektivisera leveransen av Digital Infrastruktur. Målbilden är att det ska finnas en central hubb för kod, utbildning, ramverk, moduler och kompetens som kan bistå vid utveckling relaterad till vårat produktområde.

  Modellen vi eftersträvar är NetDevOps, för att få ett så agilt och utvecklings-centriskt arbetssätt som möjligt utan att glömma att det är för optimala nätverk som arbetet sker.

- **Labb- och utbildningscenter**
  Nätverksservice utvecklar och tillhandahåller ett närverkslabb separat från VGR:s huvudsakliga nätverk där även utbildning, test och labbar med till exempel olika routingprotokoll eller liknande kan ske utan risk för påverkan på VGR:S produktionsmiljö.

  Här vill vi ge möjlighet för alla produkter inom produktområdet att testa nya versioner, buggar eller teorier i lugn och ro, kunna anordna utbildningar för sina kollegor med mera.

Säker nätverksåtkomst

Produkten Säker nätverksåtkomst omfattar de tjänster och den stödjande teknik som möjliggör att all nätverksåtkomst till och från VGR kan ske på ett kontrollerat, verifierat och säkert sätt. För att åstadkomma detta använder vi oss av ett antal olika tekniker och produkter som vi har till vårt förfogande.

Brandväggar

Vi använder brandväggar till många saker inom vårt nätverk. Det främsta användningsområdet är att skydda access till eller ifrån applikationer och system med regelverk. De används även för att identifiera användare, applikationer och system samt att blockera virus, malware och kommunikation till kända dåliga ip adresser.

De skyddar oss även ifrån olika slags hot ifrån externa källor så som denial of service attacker.

Webfilter

Webtrafik som skickas till och från internet kontrolleras och säkerhets analyseras enligt de gällande regelverk som finns på VGR. Detta ger oss möjlighet att styra bort användare ifrån osäkert innehåll på internet. Vi prenumererar på kategorier som hjälper oss att klassificera och blockera osäkert innehåll. Det vill säga websidor och applikationer som innehåller malware, virus eller annan skadlig kod.

Trafikdataloggning

All trafik som flödar i våra nätverk loggas och analyseras. Inte bara centralt när man passerar brandväggar utan även på lokala nätverk.

Intrångsdetektion och Prevention

Vi jobbar både med system för aktiv prevention av intrång samt passiva system som detekterar anomalier på nätverksnivå och rapporterar dessa till vårt övervakningsteam. Det är nätverkssystem som har flera olika slags tekniker för att detektera kända och okända hot i våra kommunikationsflöden så som signaturbaserad igenkänning samt heuristik för att upptäcka saker som tidigare inte varit kända.

Krypterade Tunnlar

När det finns behov av att ansluta externa parter eller anställda som befinner sig utanför det centrala nätverket används krypterade tunnlar. Det finns flera olika tekniker, men de vanligaste användningsområdena är "point to point" tunnlar för att ansluta partners och vissa leverantörer, samt användar-VPN för att ansluta anställda.

Nätverksinloggning

För att säkerställa att endast betrodd utrustning får lov att anslutas till våra nätverk nyttjar vi inloggningsteknik för att verifiera och säkerställa att det som ansluts lever upp till de policys som finns. gällande. I dagsläget är detta endast aktivt på delmängder av vårat nätverk, men det jobbas aktivt med att sprida detta till alla delar av nätverket.

Segmentering

De applikationer eller system som har krav på att inte samexistera på nätverket med andra system och applikationer segmenteras i egna nätverkssegment. Detta medför att vi kan på ett bättre sätt skapa förutsättningar för att endast de som skall komma åt systemet gör så, samt att systemet endast kan kommunicera med det som är bestämt enligt gällande regelverk.

Identitet och åtkomst

Produktområde Identitet och åtkomst ansvarar för de förmågor och tjänster samt den information och infrastruktur som väver ihop verksamheternas behov av masterdatahantering och uppföljning av identiteter, behörigheter och organisationstillit samt användarens behov av att kunna logga in och få åtkomst till e-tjänster och digitala underskrifter.

De lösningar och tjänster som erbjuds inom Identitet och åtkomst utgår ifrån RIV TA Anvisningar och de nationella referensarkitekturer som är framtagna av Inera, bland andra:

- Referensarkitektur för Identitet och Åtkomst.
- Referensarkitektur för elektronisk underskrift och stämpel.
- Referensarkitektur för grunddata och katalog.

Identifiering och åtkomst

Produkten Identifiering och åtkomst omfattar de förmågor, tjänster och infrastruktur som hanterar e-legitimation, organisationstillit, identifiering, åtkomstkontroll och underskrift.

E-tjänster som har behov av att lita på en organisation eller en identitet (person, utrustning, tjänst) eller som har behov av elektronisk underskrift ska kunna använda de centrala komponenterna inom produkten Identifiering och åtkomst.

Förmågor

Produkten Identifiering och åtkomst tillhandahåller ett antal förmågor:

- Utfärda och återkalla e-legitimation för personer, tjänster och utrustning.
- Verifiera identitet och utfärda identitetsintyg.
- Säkerställa användarens identitet via någon autentiseringsmetod.
- Kontrollerar begäran mot åtkomstregelverk och utfärdar åtkomstintyg.
- Tillit över organisationsgränser för informationsutbyte.

Stödjande tjänster

Produkten Identifiering och åtkomst byggs upp av ett antal samverkande tjänster:

- **E-legitimationstjänst**
  Tillhandahåller e-legitimation. Exempelvis VGR PKI.

- **Identifieringstjänst**
  Tillhandahåller funktion för identifiering. Exempelvis VGR AD och Lokal IdP.

- **Autentiseringstjänst**
  Tillhandahåller funktion för autentisering. Exempelvis Azure MFA och Inera Autentisering.

- **Åtkomstintygstjänst**
  Tillhandahåller åtkomstintyg. Exempelvis VGR AD och Lokal IdP.

- **Federationstjänst**
  Tillhandahåller federation. Exempelvis Sambi och Azure AD B2B.

- **Underskriftstjänst**
  Tillhandahåller funktion för elektronisk underskrift. Saknas idag.

- **Inloggningshjälpstjänst**
  Tillhandahåller inloggningshjälp via central lösenordshantering. Exempelvis Imprivata OneSign inom Förenklad åtkomst.

- **Regelverkstjänst**
  Tillhandahåller funktion för åtkomstregler. Exempelvis Conditional Access.

- **Åtkomstkontrollstjänst**
  Tillhandahåller funktion för åtkomstkontroll. Exempelvis F5 ADC och SiteMinder.

- **Priviligierad åtkomstkontrolltjänst**
  Tillhandahåller åtkomstkontroll för priviligerad åtkomst. Saknas idag.

Digitala arbetsflöden

Digitala arbetsflöden (leverantören som står bakom plattformen heter ServiceNow) är ett produktområde som levererar plattform med utbredd användning inom VGR. Plattformen hanterar olika typer av arbetsflöden som till stor del är automatiserade för att förbättra den operativa effektiviteten (automatisering av rutinmässiga arbetsuppgifter).

Produktområdet hanterar uppgifter, aktiviteter och processer inom en rad områden. Det skapar möjligheter för ärendehantering (incident, beställning), e-handel, rapportering, projekt, behov med mera. Produkter inom området ger information för att diagnostisera och åtgärda problem samtidigt som beroendet av kalkylblad och e-postmeddelanden tas bort.

Idag arbetar stora delar av verksamheten i plattformen på daglig basis.

Digitala arbetsflöden är indelad i ett antal områden:

- Ärendehantering IT
- Ärendehantering för service & support
- Portal & självservice
- Instyrning & projekt
- Inventarier & konfiguration
- Drift & övervakning

Ett antal integrationer säkerställer kommunikation via integrationer med andra parter för att skapa möjligheter för uppföljning av ärenden. Ett exempel är den för garantiärenden till leverantören för datorer, ett annat en incidentintegration till den leverantör som ansvarar för digitala vårdmöten. Integrationerna är uppsatta via den Regionala Tjänsteplattformen (RTJP).

Digitala arbetsflöden förhåller sig till principer och förhållningssätt uttryckta i regionens digitaliseringspolicy (RS 2020-01720) med målet att

- förenkla användarens vardag genom att minska den administrativa bördan.
- skapa nya tjänster och lösningar som är enkla, intuitiva och inkluderande.
- automatisera och standardisera för att uppnå ökad effektivitet, produktivitet, kvalitet och repeterbarhet.

Plexus (ServiceNow)

Produkten Plexus som tjänst erbjuder IT-tjänsteplattformen (ITSM-plattformen) Plexus som stöd för koncernstab digitaliserings uppdrag och leveransprocess. Tjänsten Plexus är baserad på ServiceNow och utgör ett kärnsystem för IT-verksamheten.

Plexus är indelad i ett antal områden:

Ärendehantering IT

IT-tjänstehantering berör alla aktiviteter som har att göra med planering, byggnad, implementation, support och hantering av IT-tjänster.
Målet är att optimera leveransen av VGR:s IT-tjänster för att skapa bästa möjliga användarupplevelse för medarbetarna och leverera nytta för verksamheten.

Processer kopplade till ärendehantering IT:

- Change Management - förändringshantering
- Incident Management - incidenthantering
- Knowledge Management - kunskapshantering
- Problem Management - problemhantering
- Release Management - releasehantering
- Request Fulfillment -
- Service Level Management (SLM) - hantering av tjänstenivå

Portal & självservice

Koncernstab digitaliserings tjänstekatalog för IT-erbjudanden och IT-tjänster möjliggör för regionens verksamheter att avropa tjänster från koncernstab digitaliserings IT-utbud.
Tjänstekatalogen erbjuder ett enkelt och snabbt sätt att avropa IT-tjänster, IT-erbjudanden, support och självadministration. Tjänstekatalogen ger därmed kunden en större tillgång till ett mer sammanhållet IT-utbud.
Portal & självservice Innefattar även VGR serviceportal där man kan kontakta IT-supporten, beställa behörigheter, användarlicenser, produkter eller tjänster. Där hittar man även manualer och felsökningsguider och kan få svar på vanliga frågor.

Processer kopplade till Portal & självservice:

- Service Catalogue Management - Tjänster och tjänstekomponenter

Instyrning & projekt

Ansvarar för projekt, portfölj och beredning; vilket även innefattar tid- och resurshantering. Allt från att behov kommer in och utreds: vad får det för påverkan på hårdvara, mjukvara och nätverk – till driftsättning och tidrapportering för pågående projekt och leveranser. Samt ekonomi, tidsredovisning personal och konsulter.

Processer kopplade till instyrning och projekt:

- Service Portfolio Management - hantering av tjänsteportfölj
- Application portfolio management (APM) - livscykelhantering applikationer
- Continual Improvement Management - ständiga förbättringar

Inventarier & konfiguration

Innefattar konfigurationshantering, hantering av hårdvarutillgångar och Discovery för kontroll och överblick.

Processer kopplade till inventarier och konfiguration:

- Configuration Management - konfigurationshantering
- Hardware Asset Management

Drift & övervakning

Innefattar hantering av larm, händelser och felrapporter som stöttar trafikledning och drift med överblick över hur en händelse eller ett event påverkar den övergripande IT-miljön.
Området innefattar även certifikathantering samt stöttar plattformsövergripande förmågor som masterdatahantering, integrationer med mera.

Processer kopplade till drift och övervakning:

- Event Management - larmhantering

Ärendehantering verksamhet

Produkten Ärendehantering verksamhet erbjuder en IT-tjänsteplattform för digitalisering av administrativa flöden och består idag av tjänsten Ärendehantering för service & support, ÄSS.

Ärendehantering för service & support

Tjänsten är en del av IT-tjänsteplattformen Plexus som bygger på ServiceNow och är en tjänst för hantering av administrativa ärenden.

Tjänsten riktar sig till de verksamheter som dagligen hanterar administrativa ärenden via till exempel pappersdokumentation, Excel och funktionsbrevlådor. ÄSS ger bland annat stöd för att strukturera ärenden, följa upp och kommunicera mellan handläggare och slutanvändare. Detta sammantaget bidrar till digitaliseringen av Västra Götalandsregionen.

Förväntade effekter:

- Hanteringstid för administrativa ärenden minskar
- Arbetssätt kan standardiseras och effektiviseras
- Utdaterade system kan ersättas
- Tydliga kontaktvägar och ökad transparens i ärendets livscykel
- Högre kvalitet på indata ger effektiv ärendehantering
- Strukturerad uppföljning med kvalitativa data och kraftfullt rapportverktyg möjliggör planering och styrning av resurser

Cybersäkerhet

Cybersäkerhet är en av de viktigaste frågorna för VGR idag. Med ökad digitalisering och användning av teknologi har även hoten mot VGR:s säkerhet ökat.

VGR skyddar sig mot cyberattacker med stöd av robusta säkerhetslösningar inom SIEM, endpointskydd, sårbarhetsskanning och penetrationstester.

Idag består produktområdet av:

- Säker Logghantering (SIEM Security Information och Event Management)
- Endpointskydd
- Sårbarhetsskanning
- Penetrationstester

SIEM är en säkerhetslösning som övervakar och analyserar loggdata från olika källor i realtid för att identifiera potentiella säkerhetshot. Endpointskydd är en annan viktig säkerhetslösning som skyddar organisationens enheter från olika hot. Sårbarhetsskanning är en process för att identifiera sårbarheter i organisationens system och applikationer. Penetrationstester är en mer avancerad säkerhetsmetod som involverar att en professionell testare försöker att hacka sig in i organisationens nätverk eller applikationer för att upptäcka sårbarheter och potentiella hot.

Att använda en kombination av dessa säkerhetslösningar är avgörande för att skydda VGR från cyberattacker. Det är också viktigt att våra säkerhetslösningar är uppdaterade och konfigurerade på rätt sätt för att minimera risken för intrång.

Säker endpoint

Produktområdet Säker endpoint är en tjänst som syftar till att skydda slutpunkterna i ett nätverk mot säkerhetsrisker. En slutpunkt kan vara en dator, mobiltelefon, server eller annan enhet som har en unik IP-adress och är ansluten till nätverket.

Tjänsten övervakar kontinuerligt slutpunkterna i nätverket och identifierar eventuella hot eller säkerhetsrisker som kan utgöra en fara för systemets säkerhet. Tjänsten använder olika tekniker för att identifiera hot, inklusive signaturbaserad och beteendebaserad detektion, samt maskininlärning och artificiell intelligens.

När hot upptäcks vidtar tjänsten omedelbart åtgärder för att skydda systemet. Det kan innefatta att blockera åtkomst till hotade filer, att isolera hotade enheter från resten av nätverket eller att stänga av hotade applikationer.

Säker endpoint kan också skydda mot andra hot som ransomware, virus och skadlig kod. Tjänsten uppdaterar sig själv kontinuerligt med den

senaste säkerhetsinformationen för att säkerställa att systemet alltid är skyddat mot de senaste hoten.

Sammanfattningsvis är säker enpoint en viktig tjänst för att skydda slutpunkterna i ett nätverk mot säkerhetsrisker och hot. Det ger VGR en hög grad av säkerhet och trygghet när det gäller att hantera känslig information och data.

Säkerhetsloggplattform

Produkten Hantering av säkerhetsloggar omfattar Security Incident Event Management, förkortat SIEM fortsättningsvis, är en teknik som används vid hotdetektering, efterlevnad och hantering av säkerhetsincidenter.

Genom insamling och analys av säkerhetshändelser, både i realtid och historiskt data, samt en mängd andra händelser och kontextuella datakällor används SIEM systemet vid säkerhetsincidenter.

Västra Götalandsregionens IT-enhet har som samhällsuppgift att skydda medborgarnas informationstillgångar. Detta uppdrag försvåras genom ständiga IT attacker mot regionens infrastruktur och informationstillgångar.

Som del av säkerhetsarkitekturen för att skydda informationstillgångar i Västra Götalandsregionen, har ett beslut fattats om att synliggöra hot mot IT infrastrukturen.

SIEM systemet är en del av denna säkerhetsarkitektur. Västra Götalandsregionen har ett Cybersäkerhetcenter som nyttjar SIEM systemet för att lösa den ålagda samhällsuppgiften och att synliggöra hotbilder.

Cybersäkerhetcentret ska i SIEM systemet ha förmågan att samla, analysera och presentera information från bland annat:

- nätverks- och säkerhetsenheter
- identitets- och åtkomsthanteringsapplikationer
- sårbarhetshantering och kontroll av följsamhet mot policies
- operativsystem, databas och applikationsloggar
- externa hot

Fler datakällor tillkommer fortlöpande i och med att Cybersäkerhetcentrets arbete utvecklas över tid.

Den tänkta lösningen för SIEM skall tillgodose de behov som Cybersäkerhetscentret har på verktyget i första hand. Även en bredare konsumtion av kapabiliteterna i SIEM verktyget kan erbjudas till verksamheten utanför enheten Infrastruktur och cybersäkerhet.

Sårbarhetsskanning och penetrationstest

Produktområdet sårbarhetsskanning och penetrationstest omfattar de två tjänster som VGR erbjuder inom området, och innefattar följande:

Sårbarhetsskanningstjänst

VGR:s sårbarhetsskanningstjänst är en automatiserad tjänst som används för att identifiera sårbarheter i IT-system och webbapplikationer. Tjänsten utför en grundlig skanning av nätverksportar och protokoll för att upptäcka exponerade sårbarheter i systemet. Sårbarheterna kategoriseras och prioriteras efter deras allvarlighetsgrad. En detaljerad rapport genereras och levereras till kunden som visar de identifierade sårbarheterna och ger rekommendationer för hur de kan åtgärdas.

Penetrationstestningstjänst

VGR:s penetrationstestningstjänst är en manuell tjänst som syftar till att testa IT-system och webbapplikationer för att upptäcka och exploatera sårbarheter. Tjänsten innefattar ett simulerat angrepp av en erfaren testare på systemet för att identifiera eventuella säkerhetsproblem. Testerna utförs för hand för att simulera en verklig attacker och inkluderar social ingenjörskonst, avancerade nätverksattacker och applikationslagerattacker. En detaljerad rapport levereras till kunden som visar de upptäckta sårbarheterna, deras allvarlighetsgrad och rekommendationer för åtgärdande åtgärder.

Beställning av sårbarhetsskanning

Sårbarhetsskanning kan beställas av ansvarig tjänsteägare eller systemförvaltare via e-tjänsteportalen i ITSM-verktyget Plexus.

Styrning och ledning

Koncernstab digitalisering

Koncernkontoret arbetar med regionövergripande frågor inom bland annat hälso- och sjukvård, regional utveckling, ekonomi, personal/HR, digitalisering/IT och information/kommunikation.

Koncernstab digitalisering är en del av koncernkontoret med uppdrag att stötta och driva digitalisering av VGR:s verksamhet samt territoriet Västra Götaland, utveckla nya digitala arbetssätt samt implementera nya digitala lösningar. Koncernstaben har också ett grundläggande uppdrag och ansvar att erbjuda stabil och säker IT-plattform samt effektiv drift, support, förvaltning och utveckling av både nya och befintliga system.

Koncernstabens arbete utgår från de regionövergripande styrdokument som beslutas av regionfullmäktige, och organiseras linjemässigt och funktionellt med utgångspunkt i VGR:s ordinarie ledningssystem.

IT- och verksamhetsarkitektur inom VGR

Inom koncernstab digitalisering finns en sammanhållen arkitekturfunktion med etablerade roller och gemensamma arbetssätt, metoder och verktyg för arkitekturarbete.

Arkitekturfunktionen erbjuder arkitekturstöd, vägledning och kvalitetssäkring som stöd åt strateger, utvecklings- och förvaltningsansvariga samt andra intressenter både inom och utanför koncernstaben.

Det finns även hela etablerade arkitekturfunktioner och viss förmåga till framför allt verksamhetsarkitektur inom andra koncernstaber, förvaltningar och bolag, till exempel inom Västtrafik AB och koncernstab kansli och säkerhet.

Mer information

- För mer information om VGR:s styrande dokument, läs här: Aktuella styrande dokument - Västra Götalandsregionen
- För mer information om Koncernkontoret, läs här: Koncernkontoret - Västra Götalansregionen
- För mer information om koncernstab digitalisering, läs här: Koncernstab digitalisering - Västra Götalandsregionen
- För mer information om koncernstab kansli och säkerhet, läs här: Koncernstab kansli och säkerhet - Västra Götalandsregionen
- För mer information om Västtrafik AB, läs här: Om Västtrafik AB

Styrande dokument

Styrande dokument är ett av Västra Götalandsregionens viktigaste verktyg för ledning och styrning. För att beslut och initiativ ska få genomslag i verksamheterna är det viktigt att de kan omsättas i agerande – styrande dokument utgör ett stöd för chefer och medarbetare att agera på rätt sätt. Styrande dokument kan vara allt ifrån en policy med övergripande politiska mål till en detaljerad rutin i ett specifikt vårdförlopp.

För att uppnå styrdokumentens inriktning och mål krävs prioritering av insatser och resurser. Det är regionfullmäktiges årliga budget som styr denna resursfördelning, vilket innebär att budgeten är det överordnade styrdokumentet. I praktiken innebär det att målen i enskilda styrdokument kan komma att prioriteras ned till förmån för specifika insatser utifrån regionfullmäktiges budget.

Styrande dokument är en del av Västra Götalandsregionens ledningssystem. Läs mer om ledningssystemet här: Västra Götalandsregionens ledningssystem

Aktuella regionala styrdokument

Regionövergripande styrdokument gäller samtliga styrelser, nämnder, förvaltningar och bolag inom Västra Götalandsregionen. För att ett styrdokument ska gälla hela Västra Götalandsregionen inklusive bolag måste det beslutas av regionfullmäktige.

Här följer ett urval av styrdokument med särskild betydelse för utvecklingen av VGR:s IT-miljö:

Vision

Vision Västra Götaland är Västra Götalandsregionens och de 49 kommunernas gemensamma vision. Visionen uttrycker det önskade framtida tillståndet som vi vill nå - Det goda livet.

- Vision Västra Götaland - Det goda livet

Måldokument

Västra Götalandsregionen har fyra måldokument som anger mål som ska bidra till att uppfylla visionen – Det goda livet. Flera av dokumenten har Västra Götalandsregionen tagit fram tillsammans med kommuner, kommunalförbund och andra berörda parter, som statliga verk, högskolor och universitet och den ideella sektorn.

- Strategi för omställningen av hälso- och sjukvården i Västra Götalandsregionen 2023 - 2027
- Regional utvecklingsstrategi för Västra Götaland 2021–2030
- Västra Götalands kulturstrategi och kulturplan 2024–2027
- Trafikförsörjningsprogram 2021-2025 - Hållbara resor i Västra Götaland

Västra Götalandsregionens budget

Budgeten är vårt viktigaste styrande dokument där mål och fokusområden prioriteras på 1-3 års sikt och där ekonomiska förutsättningar ges för att bedriva vår verksamhet inom hälso- och sjukvård och regional utveckling.

- Budget

Digitalisering

Regionens digitaliseringspolicy har som syfte att vägleda verksamhetens digitalisering genom ett antal principer och förhållningssätt.

- Digitaliseringspolicy

Miljö och hållbarhet

Västra Götalandsregionens (VGR) miljöpåverkan och resursanvändning är betydande. Miljömål 2030 är ett viktigt styrdokument för alla som arbetar inom VGR. Miljö, hälsa och ekonomi hänger ihop. Med stöd av vår miljöpolicy, tydliga delmål och konkreta åtgärder kan vi tillsammans skapa ett gott liv – för oss och för kommande generationer.

- Miljömål 2030
- Agenda 2030

Övriga styrande dokument

En komplett lista över styrande dokument återfinns på VGR:s webbplats.

- Läs mer om dessa här:
  Aktuella regionala styrande dokument