OFFENTLEG

STYREMØTE I
HELSE VEST IKT

HELSE VEST IKT

INNKALLING TIL STYREMØTE
HELSE VEST IKT

STAD: **Teams**
MØTETIDSPUNKT: **Torsdag 13. juni, kl. 08:30 – 11:30**

GÅR TIL:

Styremedlemmer

Anders Hovland	Medlem
Helle Kristine Schøyen	Medlem
Beate Sander Krogstad	Medlem
Arve Varden	Medlem
Eivind Gjemdal	Medlem
Eivind Hansen	Medlem
Stian Hoell	Medlem
Agnete Sjøtun	Medlem
Silje Ljosland Bakke	Medlem
Merethe Nygård	Medlem

Styremøte er ope for publikum og presse

Stavanger, 06.06.2024
Helse Vest IKT

Inger Cathrine Bryne
Styreleiar

SAKSLISTE:			**UNDERLAG:**
		OPNE SAKER	
Sak	22/24 B	Godkjenning av innkalling og dagsorden	Vedlagt
Sak	23/24 B	Protokoll frå styremøte i Helse Vest IKT AS 26.04.2024	Vedlagt
Sak	24/24 O	Administrerande direktør si orientering	Vedlagt
Sak	25/24 B	Rapport frå verksemda april 2024	Vedlagt
Sak	26/24 O	Fornya vurdering av oppseiing Blå Kors	Vedlagt
Sak	27/24 O	Rapportering på bruk av ITIL rammeverk	Vedlagt
Sak	28/24 B	Innkalling til ordinær generalforsamling Helse Vest IKT AS	Vedlagt
Sak	29/24 O	Trusselvurdering spesialisthelsetjenesten 2024	Vedlagt
		LUKKA SAKER	
Sak	30/24 O	Leverandørrisiko for sentrale leverandørar	Vedlagt
Sak	31/24 O	Mogleg handlingsrom for regional løysing for kurve og legemiddelhandtering	Vedlagt
Sak	32/24	Eventuelt	
		Styret sitt kvarter	

HELSE VEST IKT

PROTOKOLL FRÅ STYREMØTE I HELSE VEST IKT AS

STAD: Teams
MØTETIDSPUNKT: 26.04.2024, 12:30 – 15:00

Styremøte var ope for publikum og presse

DELTAKARAR FRÅ STYRET
Inger Cathrine Bryne
Helle Kristine Schøyen
Anders Hovland
Beate Sander Krogstad
Arve Varden
Eivind Gjemdal
Eivind Hansen
Stian Hoell
Agnete Sjøtun
Silje Ljosland Bakke
Merethe Nygård

FORFALL FRÅ STYRET

DELTAKARAR FRÅ ADMINISTRASJONEN
Ole Jørgen Kirkeluten
Harald Flaten
Ørjan Andersen
Vidar Råheim
Gjertrud Fagerli
Fredrik Eldøy
Kristin Farestvedt
Ole Fredrik Gulbrandsen
Leif Nordland

Aksel Bruun, CISO Helse Vest IKT deltok i sak 020/24 B

Møtedokumentet er elektronisk godkjent og har ikkje handskrivne signaturar

Postadresse:
Helse Vest IKT AS
Inndalsveien 12
5052 Bergen

Elektronisk adresse:
postmottak@helse-vest-ikt.no
www.helse-vest-ikt.no

Besøksadresse:

Generell informasjon:
Sentralbord 55 97 65 00
Org.nr: 987 601 787

Saksliste:

		Opne saker
Sak	13/24 B	Godkjenning av innkalling og dagsorden
Sak	14/24 B	Protokoll frå styremøte i Helse Vest IKT AS 14.03.2024
Sak	15/24 O	Administrerande direktør si orientering
Sak	16/24 B	Rapport frå verksemda mars 2024
Sak	17/24 B	Økonomisk langtidsplan 2025 - 2029
Sak	18/24 O	Forbetringsundersøkelsen 2024
Sak	19/24 O	KI-tenesta i Helse Vest IKT
		Lukka saker
Sak	20/24 B	Leiinga sin gjennomgang IKT-sikkerheit
Sak	21/24	Eventuelt
		Styret sitt kvarter

Postadresse:
Helse Vest IKT AS
Inndalsveien 12
5052 Bergen

Elektronisk adresse:
postmottak@helse-vest-ikt.no
www.helse-vest-ikt.no

Besøksadresse:

Generell informasjon:
Sentralbord 55 97 65 00
Org.nr: 987 601 787

HELSE VEST IKT

Opne saker

Sak 13/24 B **Godkjenning av innkalling og dagsorden**

Vedtak (samrøystes):
1. Styret godkjente innkalling og dagsorden.

Sak 14/24 B **Protokoll frå styremøte i Helse Vest IKT AS 14.03.2024**

Vedtak (samrøystes):
1. Styret godkjente protokoll frå styremøtet 14.03.2024.

Sak 15/24 O **Administrerande direktør si orientering**

1. Datahall i Bergen

Helse Vest IKT vil i løpet av Q1/Q2 2025 flytta ut av datahallane i IT-bygget og sentralblokka på Haukeland sjukehus, og inn i ny datahall som støttar dagens sikkerheitskrav.

2. «Pasientens journaldokument» har vunne årets eHelsepris

Helse Vest har leia arbeidd med nasjonal delingsteneste for journaldokument og prøvesvar. eHelseprisen er ei flott anerkjenning av det gode arbeidet som er lagt ned i Helse Vest.

3. Smidige leveransar og tverrfagleg samarbeid i team

Styrings- og områdestrukturen for digitalisering i Helse Vest legg opp til at me i aukande grad skal arbeida meir smidig i leveransane. Teamorganisering og fokus på teamarbeid blir dermed relevant for tida framover. OU-teamet i Helse Vest IKT har til dømes utarbeid innføringskurs for alle tilsette i smidig tankesett og teamarbeid/teamorganisering (Team topology).

4. Sikkerheitsutfordringar i applikasjonar

Aktuelle sikkerheitsutfordringar og tiltak i samanheng med disse vart orientert om i møtet.

5. Rapportering tilsynssaker

Ingen aktuelle saker

6. Orientering om relevante lover, forskrifter og myndigheitskrav

Ingen aktuelle sakar

Postadresse:
Helse Vest IKT AS
Inndalsveien 12
5052 Bergen

Elektronisk adresse:
postmottak@helse-vest-ikt.no
www.helse-vest-ikt.no

Besøksadresse:

Generell informasjon:
Sentralbord 55 97 65 00
Org.nr: 987 601 787

7. Oversikt over aktuelle høyringar

Ingen aktuelle sakar

Vedtak (samrøystes):

1. Styret tok saka til orientering

Sak 16/24 B

Rapport frå verksemda mars 2024

Driftskalenderen for mars viser 5 Omfattande Episodar med beredskap i mars. Vi hadde 2 gule og 3 grøne tilfelle med beredskap. 14.mars var det problem med DECT telefonar på Haukeland Universitetssjukehus og her vart det ikkje utløst Grøn beredskap, men i retrospekt skulle vi gjort det så derfor tar vi den med på kalenderen.

Det vart i mars rapportert 118 «moglege sikkerheitsavvik» i Helse Vest IKT sitt sakshandsamingssystem, ei auke frå februar. Ein stor del av disse var knytt til automatiserte varsel.

Økonomisk resultat er dårlegare enn venta med eit resultat per mars på -6,9 mill. kr., eit avvik mot budsjett på 10,4 mill.kr. Avviket skuldast i hovudsak for lite timar levert til investeringsprosjekt. Det er sett i verk tiltak for å redusere kostnadar.

Sjukefråvær er framleis høgare enn ønska med 6,1%, men det er ei positiv utvikling i 2024 med lågare fråvær enn i 2023. Turnover er også noko høgare enn ønska med 6,2%.

Vedtak (samrøystes):

1. Styret tok saka til etterretning.

Sak 17/24 B

Økonomisk langtidsplan 2025 - 2029

Viser til sak 009-24 O der administrasjonen la fram ei løypemelding for arbeidet med økonomisk langtidsplan for 2025 – 2029.

I arbeidet med økonomisk langtidsplan er ny utviklingsplan (ref styresak 065/23) lagt til grunn for ambisjonar og målbilete, og for å lukkast med måla er mellom anna disse tiltaka prioritert:

- Digital plattform som legg til rette for tenester og automatiserte prosessar for utvikling, mellom anna til autentisering, sanntidshub, API
- Legge til rette for mobile løysingar og app'ar
- Phising resistent autentisering ved bruk av sikkerheitsnøkkel (FIDO2)

- Mikrosegmentering og software defined access på nettverk
- Utnytte moglegheit i M365
- Etablere plattform for Kunstig intelligens
- Forbetring i yting, kortare påloggingstid og mindre «plunder og heft»

Framlegget til økonomisk langtidsplan er Helse Vest IKT sitt beste overslag over våre kostnader for perioden 2025 – 2029, alt i 2024-kroner og utan justeringar for pris og lønsvekst i perioden.

Styret kommenterte at det er svært krevjande med den kostnadsveksten ein har innanfor IKT, og det er viktig at ein i samarbeid med HF'a gjer gode prioriteringar, er kostnadseffektiv, har fokus på automatisering, samtidig som ein bidreg til auka nytte og redusert ressursbruk i HF'a. Dersom den økonomiske situasjonen i føretaksgruppa krev det, kan sum digitalisering i økonomisk langtidsplan bli justert ned frå 2027 ved neste års handsaming av økonomisk langtidsplan.

Vedtak (samrøystes):

1. Styret vedtok økonomisk langtidsplan for 2025 - 2029.

2. Styret bad Helse Vest IKT vidareføre arbeidet med å redusere kostnadar og bemanningsauke i langtidsperioden.

3. Eventuelle endringar i ramme for digitalisering vedtatt i Digitaliseringsstyret innarbeidast i økonomisk langtidsplan i etterkant.

Sak 18/24 O **Forbetringsundersøkelsen 2024**

85,27 % av medarbeidarar i Helse Vest IKT har svart på ForBetrings-undersøkinga i 2024. I 2023 var svarprosenten 87.
Overordna viser undersøkinga stabilt gode resultat for Helse Vest IKT.
Resultata er tilgjengeleg for alle tilsette, dermed og for verneombud og tillitsvalde i Helse Vest IKT.
Undersøkinga vert gjennomgått og fulgt opp i dei enkelte avdelingar og seksjonar utover våren/sommaren. Det er leiar som har ansvar for å dele og følgje opp resultata i si eining.

Vedtak (samrøystes):

1. Styret tok saka til orientering.

Sak 19/24 O **KI-tenesta i Helse Vest IKT**

KI-tenesta i Helse Vest IKT presenterte status og planlagt aktivitet.

Vedtak (samrøystes):

1. Saka vart utsett til neste styremøte.

Lukka saker

Sak 20/24 B

Leiinga sin årlege gjennomgang av informasjonssikkerheit og personvern for Helse Vest IKT AS 2023

Leiinga sin årlege gjennomgang skal gjere verksemda sitt styre, direktør og leiing i stand til å gjere dei rette prioriteringane i arbeidet med førebyggande sikkerheit, informasjonssikkerheit og personvern. Visjon og prinsipp for informasjonssikkerheit i Helse Vest IKT er definert i overordna informasjonssikkerheitspolicy for Helse Vest IKT.

Styret i Helse Vest RHF vedtok i styresak 084/21 den 30.09.2021 Regional handlingsplan for informasjonssikkerheit. Arbeidet med den regionale handlingsplanen har fortsett i 2023, og prosjekta har levert konkrete resultat i form av anbefalingar, utprøving av konsept, revisjon av regional malverk for styringssystem og tekniske pilotar.

Administrasjonen er av det syn at utviklinga innanfor IKT-sikkerheit er tilfredsstillande. Samstundes vil administrasjonen understreke at det er særs viktig å vidareføre arbeidet med tiltak foreslått i vedlegg 1.

Styret kommenterte at det er viktig å sjå arbeidet med tiltak for informasjonssikkerheit saman med regional handlingsplan.

Vedtak (samrøystes):

1. Styret tok rapporten «Årleg gjennomgang av informasjonssikkerheit og personvern for Helse Vest IKT AS» til etterretning.

Sak 21/24

Eventuelt

Ingen saker

HELSE VEST IKT

Postadresse:
Helse Vest IKT AS
Inndalsveien 12
5052 Bergen

Elektronisk adresse:
postmottak@helse-vest-ikt.no
www.helse-vest-ikt.no

Besøksadresse:

Generell informasjon:
Sentralbord 55 97 65 00
Org.nr: 987 601 787

STYRESAK

GÅR TIL: Styremedlemmer
FØRETAK: Helse Vest IKT AS

DATO: 06.06.2024
FRÅ: Administrerande direktør
SAKSHANDSAMAR: Ole Jørgen Kirkeluten
SAKA GJELD: **Administrerande direktør si orientering**

ARKIVSAK:
STYRESAK: **024-24 O**

STYREMØTE: 13.06.2024

FORSLAG TIL VEDTAK

1. Styret tek saka til orientering.

OPE DEL

1. **Ny teknisk plattform Libra**
   Helse Vest IKT har i løpet av 25 – 26. mai migrert Libra til ny teknisk plattform, sjå vedlegg 1.

2. **Oppgradering Dips Arena**
   Helse Vest IKT har i løpet av 25 – 26. mai oppgradert Dips til ny versjon, sjå vedlegg 2.

3. **Oppgradering Meona**
   Helse Vest IKT har i løpet av 5. juni oppgradert Meona til ny versjon, sjå vedlegg 3.

4. **Oppgradering Sectra**
   Munnleg orientering

5. **Kulturkartlegging Helse Vest IKT**
   Munnleg orientering

6. **Rapportering tilsynssaker**
   Ingen aktuelle sakar

7. **Orientering om relevante lover, forskrifter og myndigheitskrav**
   Ingen aktuelle sakar

8. **Oversikt over aktuelle høyringar**
   Ingen aktuelle sakar

LUKKA DEL

9. **Ingen aktuelle sakar**

HELSE VEST IKT

Prosjekt SOLID

Orientering styre

Prosjekt SOLID har flytta LIBRA til ny driftspartner våren 2024

Då LIBRA stod på ein utgåande serverpark var det nødvendig å sjå på nye løsninger for vidare drift. Det ble gjort analyser av forskjellige driftsmodellar, og det blei beslutta å inngå kontrakt med ein leverandør av både infrastruktur og SAP Basis drift. Det inneber at leverandøren står for investering i ny serverpark.

Formålet med prosjektet

Helse Vest IKT skal ha ein solid driftspartnar som sørger for at LIBRA er på ein moderne digital plattform med høg sikkerhet.

Gevinstar prosjektet har jakta på:

- Auka sikkerheit, tilgjengeligheit og stabilitet
- Forbetra yting
- Senka tidsforbruk på oppfølging av leverandør ved å tilknytta seg en proaktiv og solid driftspartner

Det viktigaste resultatmålet til prosjektet:
Prosjektet skal migrere alle SAP-systemer på vår plattform til ein ny driftsleverandør før juli 2024. Det skal ikkje innførast nokon funksjonelle endringer.

Tidslinje

Prosjektet må vere ferdig før juli 2024 fordi serverane då ikkje lengre har driftsavtale.

- **Mai 2023:**
  Svar på RFI viste gode indikasjoner på markeds- og leverandørsituasjonen
- **Juni 2023:**
  Utsendelse av konkurranse
- **Oktober 2023:**
  Signering av kontrakt med Basis Consulting
- **Mai 2024:**
  Migrering av LIBRA ferdigstilt i god tid før driftsavtale på gammal plattform utgår

Prosjektet har blitt eigt og leidd av LIBRA forvaltning med støtte frå foretak

- Fire vekers UAT med over 60 involverte testressursar frå foretak og LIBRA forvaltning.
- Cirka 100 involverte personer frå både Helse Vest IKT, foretak og leverandørane under go-live helg.

Resultat så langt

- Opplever forbetra yting og raskare respons på systemet.
- Oppgradert til eit høgare sikkerheitsnivå
- Opplever godt samarbeid mellom leverandørane og Helse Vest IKT

Etter en intens produksjonssettingshelg så ser det ut som at dette har gått veldig bra og jeg er stolt av alle i foretakene og Helse Vest IKT som har gjennomført et Solid prosjekt for oppgradering av teknisk plattform for LIBRA til glede for alle brukerne på Vestlandet.
-Per Karlsen, områdeeier økonomi og forsyning

Oppgradering av DIPS 25 mai 2024

- Ny versjon av DIPS Arena
- Ny versjon av DIPS Classic
- Installere tjenester på ny tjenesteplattform (Kubernetes)

Tidsplan

Kl. 1300 – 2030 DIPS i lesemodus
Erstatningsjournal aktivert
Oppgradering av database
Installere tjenester på ny plattform (Kubernetes)

Kl. 1930 Varsler foretak om utvida nedetid
Kl. 2030 Prodtest – tekniske utfordringar
Kl. 2200 Aktiverer produksjonsmiljø
Div etterarbeid i Helse Vest IKT
Etterregistrering i foretakene
Kl. 0200 Slutt

Kva gjer vi no?

- Kontinuerlig overvåking av loggar
- Interne statusmøter i Helse Vest IKT
- Møter med foretak annakvar dag

Oppsummering

Hovudsak positive tilbakemeldingar
Ulike signal knytt til ytelse

Database:	Få problem
Kubernetes:	Ingen utfordringar
Gammal plattform:	Behov for justeringar

«Jeg snakket akkurat lenge med en av overlegene våre og når han gikk inn i Arena:
1) Opplevde han store ytelsesforbedringer
2) Spesielt fornøyd med ytelse på AOM og
3) Et endringsønske han hadde meldt var kommet med»

Anne Kristin Paulsen, lokal systemansvarlig Felles EPJ, Helse Bergen

Oppgradering til MEONA 2024.4.11
5. juni 2024

Funksjonalitet
Versjonen inneheld mange nye viktige funksjonalitetar, blant anna SOAP/REST endring til Kjernejournalen og massivt løft for datafangst som er særs etterspurt i klinikken.

Vidare framdrift og utvikling
Det er viktig å komme opp på nyare versjon av MEONA for å komme vidare med utvikling av E.care, Kjemoterapi-modul og feilretting. Denne oppgraderinga gjer at vi kjem i takt med nyaste versjon hos Mesalvo.

Feilretting
Versjonen leverer mange viktige feilrettingar, >77 stykker, blant anna 2 systemsviktsaker som er særs viktige å få retta i produksjon. Den redar også grunnen for vidare feilretting i produksjon.

De facto halvering av antall feil i produksjon med denne oppgraderinga.
Reduksjon frå 145 til 80 feil i produksjon.

Tidsplan

17:30: DEPLOY IN PROD

17:45: KONFIG i PROD

18:00: Datafangstserver installasjon * 5 føretak

18:10: Konfig ferdig - Tvungen omstart av MEONA klient

18:15: Start verifikasjonstest

22:00: Verifikasjonstest ferdig

Kva gjer vi etter oppgraderinga

- Statusmøte kl. 9 torsdag 6. juni med Prosessteam Drift og delområdeleiar
- Statusmøte med Mesalvo kl. 11 6. juni
- Early Life Support med auka årvåkenhet i 2 veker etter oppgraderingstidspunkt

Oppsummering

Vi oppgraderte ihht til tidsplan!
Ingen uforutsette hendelsar så langt.

Nokre lause trådar på datafangst som datafangst-teamet jobbar med allereie saman med Mesalvo.

Nokre få nye feil avdekka i verifikasjonstesten. Totalt 5 stykk.

Desse rapporterast til Mesalvo fortløpande, foreløbig ikkje avdekka noko som må patchast.

So far so good!

STYRESAK

GÅR TIL:	Styremedlemmer
FØRETAK:	Helse Vest IKT
DATO:	06.06.2024
SAKSHANDSAMAR:	Ole Jørgen Kirkeluten, Fredrik Eldøy, Leif Nordland
SAKA GJELD:	**Rapport frå verksemda april 2024**
ARKIVSAK:	
STYRESAK:	**Styresak 025/24 B**
STYREMØTE:	**13.06.2024**

FORSLAG TIL VEDTAK

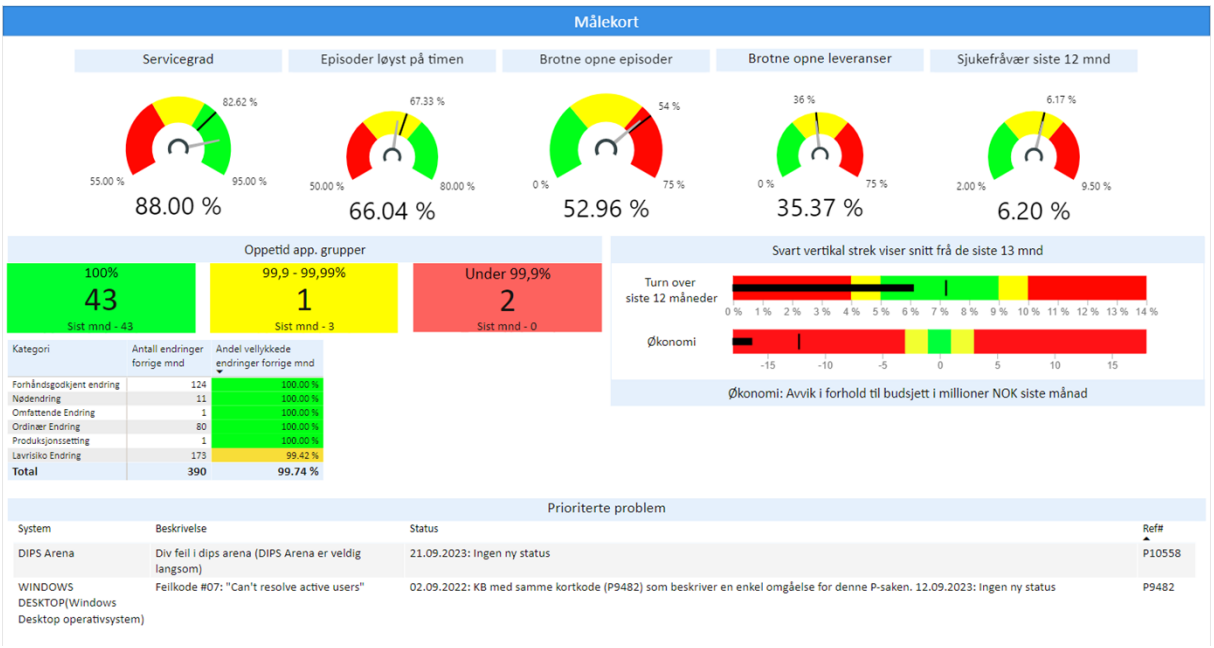
1. *Styret tek rapport frå verksemda per april 2024 til etterretning.*

Oppsummering

Administrasjonen har summert opp rapport om verksemda i ein figur som viser overordna status.

Fakta

Figuren nedanfor viser målkortet for april 2024



Kommentarar frå Administrerande direktør
Driftskalenderen for april viser 4 Omfattande Episodar med beredskap i april. Vi hadde 1 gul og 3 grøne tilfelle med beredskap. 12 april hadde vi 2 ulike OE-er same dag.

Det ble i april 2024 rapportert 80 «mulige sikkerhetsavvik» i Helse Vest IKT sitt sakshåndteringssystem, en nedgang fra mars 2024. En stor andel av disse var tilknyttet automatiserte varsler.

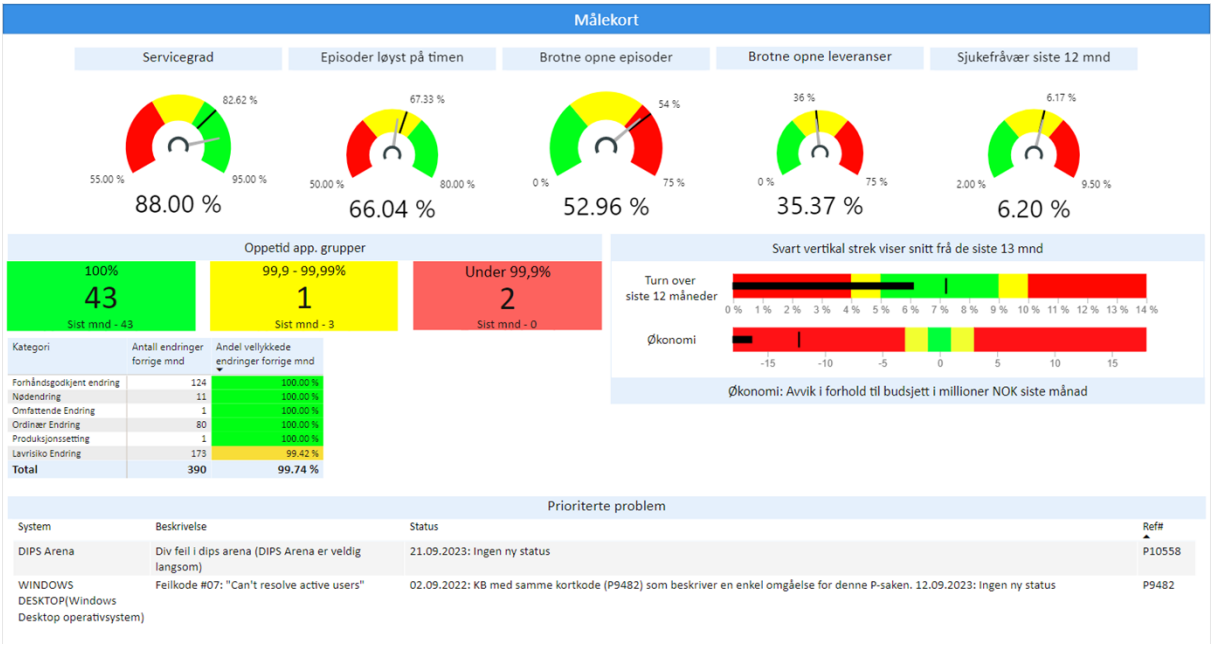
Økonomisk resultat er dårlegare enn venta med eit resultat per april på -10,9 mill. kr., eit avvik mot budsjett på 16,7 mill.kr. Avviket skuldast i hovudsak for lite timar levert til investeringsprosjekt. Det er sett i verk tiltak for å redusere kostnadar.

Sjukefråvær er framleis høgare enn ønska med 6,2%, men det er ei positiv utvikling i 2024 med lågare fråvær enn i 2023. Turnover er innanfor akseptabelt nivå med 6,1%.

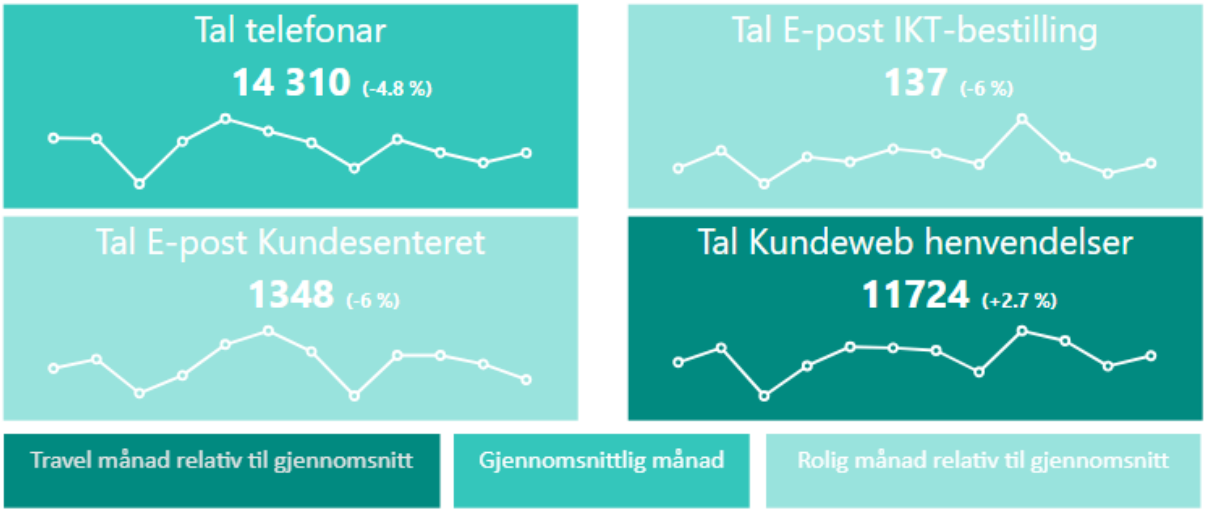
VEDLEGG STYRESAK

GÅR TIL:	Styremedlemmer
FØRETAK:	Helse Vest IKT AS
DATO:	06.06.2024
SAKSHANDSAMAR:	Fredrik Eldøy, Rolf Ruland, Leif Nordland
SAKA GJELD:	**Verksemdsrapport april 2024**
ARKIVSAK:	
STYRESAK:	**025-24 B**
STYREMØTE:	**13.06.2024**

Målkort



Produksjon



<u>Definisjonar:</u>
Her viser vi totalen for denne månaden. I parentes vises prosentavvik i forhold til gjennomsnittet de siste 13 mnd.
E-post support: Teller all e-post til Kundesenteret med unntak av spam-mail.
E-post bestilling: Teller all e-post med unntak av spam-mail som kommer inn til ikt-bestillingsadressene til Sal.
Kundeweb: Mengd oppdateringar på eksisterande saker eller nye saker.
Telefon: Mengd telefoner svara på av Kundesenteret.

HELSE VEST IKT

Loggede saker per topp 20 enheter

Berørt Enhet	Antall
DIPS Arena PROD	2784
Microsoft 365	1211
PC	1082
Leveranser av nytt IKT utstyr	795
Passord, nytt	653
OV000000218 - MEONA (KULE)	584
Ukjent/manglende programvare	529
Teams klient for pc	350
Domenepåloggingstjenesten	349
Nettverksskriver	345
RPA Robotisert Prosess Automatisering HVN PROD	335
Sikkerhet - Datakommunikasjonstjeneste (nettverk infrastruktur)	275
Imatis Fundamentum Prod	259
Forvaltning-Vedlikehold leverandør	245
MEONA HVN Produksjon (System 3)	215
Printer	201
SMS - 2-FAKTOR (RSA) HVI PROD	195
Kunnskapsprosessen (ITIL, Service Transition, Knowledge Mangement)	194
Generisk item for mobiltelefon	188
SECTRA RIS/PACS HVN PRV PROD	172

Topp 20 årsaker

Årsaksenhet produkt [Avslutt]	Antall
DIPS ARENA HVN PROD	2170
M365	1228
PC	871
PASSORD, NYTT	655
LEVERANSER AV NYTT IKT UTSTYR	503
$PROGRAMVARE, UKJENT	381
DOMENEPÅLOGGINGSTJENESTEN	373
RPA HVN PROD	335
$NETTVERKSSKRIVER	325
TEAMS KLIENT HVN PRV EXT PROD	319
BRANNMUR	318
DIPS HVN PROD	309
MEONA HVN PRV PROD: NØDPCER	296
MEONA HVN PRV PROD	280
$PC, UKJENT	269
IMATIS FUNDAMENTUM HVN HDS PROD	264
BRUKERKONTO, ENDRING	261
FORVALTNING-VEDLIKEHOLD LEVERANDØR	242
$PC TILBEHØR	225
2-FAKTOR (RSA) HVI PROD:SMS	212

Som vanlig er det DIPS Arena og M365 som topp statistikken over det Kundesenteret får flest henvendelser om.

Kategori	Instans	Diff Instans	Produkt	Diff Produkt
Laboratorie - Ytterleg	65	-2	30	-1
PAS og EPJ - Ytterleg	45	2	16	0
Røntgen - Ytterleg	33	1	18	0
SMSYS - Mellomstore	232	0	153	-1
SMSYS - Små	715	-9	596	-8
Understøttende - Desktop	57	-2	21	0
Understøttende - Nettverksapplikasjoner	75	-1	33	-1
Web portaltjenester - Ytterleg	28	1	14	1
Total	**1250**	**-10**	**881**	**-10**

Status	Link	Enhet ID	Enhet	Kategori
Bytte av kategori før		98468	Keypoint Data Center	SMSYS - Mellomstore
Ny		128271	JetBrains Datagrip	SMSYS - Små
Ny		229045	SentrySuite HST	SMSYS - Mellomstore
Ny		264059	Philips Remote Device Manager HVN Prod	PAS og EPJ - Ytterleg
Ny		268858	Lokalisering av sterilt utstyr PRODUKSJON	Web portaltjenester - Ytterleg
Ny		269534	Lunar HFD	SMSYS - Mellomstore
Ny		275707	Fina arkivering ver.2.3	Røntgen - Ytterleg
Ny		276125	Rosa Chatbot	Web portaltjenester - Ytterleg
Ny		276240	LightCycler 480	SMSYS - Små
Ny		276551	Philips Client Extensions	PAS og EPJ - Ytterleg
Utfaset		23254	SymPathy HFD v. 5.2.3.2 - Arkivløsning	Laboratorie - Ytterleg
Utfaset		24307	Cisco ACS 5.5	Understøttende - Nettverksap...
Utfaset		25055	MAPLE	SMSYS - Mellomstore
Utfaset		37461	Windows 7 x86 OS	Understøttende - Desktop
Utfaset		37462	Windows 7 x64 bits OS	Understøttende - Desktop
Utfaset		74528	WinEEG 2.90.53 (WinEEG: QEEG and ERP a...	SMSYS - Små
Utfaset		74532	EEG Studio	SMSYS - Små
Utfaset		94080	Datalogger 4.1	SMSYS - Små
Utfaset		102206	SSI Lisrel	SMSYS - Små
Utfaset		116269	Prosjektweb HVI PROD	Web portaltjenester - Ytterleg
Utfaset		119572	Keypoint Classic	SMSYS - Små
Utfaset		121711	Unified Mass Spectroscopy Control Databa...	Laboratorie - Ytterleg
Utfaset		121775	officeweb.helse-vest.no office online server	Web portaltjenester - Sharep...
Utfaset		144390	Intendu - Functional Brain Trainer	SMSYS - Små
Utfaset		188281	Genie Modeler academic fra BayesFusion.c...	SMSYS - Små
Utfaset		188893	Cygnet 2.0.5	SMSYS - Små
Utfaset		189970	Sisulizer	SMSYS - Små
Utfaset		190486	KI Box	SMSYS - Små
Utfaset		226826	VirSEAK	SMSYS - Mellomstore
Utfaset		237918	E4 Manager	SMSYS - Små

Driftskalender

Driftskalenderen for april viser 4 Omfattende Episoder med beredskap. Vi hadde 1 gul og 3 grønne beredskaper. 12.april hadde vi 2 ulike OE-er samme dag.

April 2024

Mandag	Tirsdag	Onsdag	Torsdag	Fredag	Lørdag	Søndag
1	2	3	4	5	6	7
8	9	10	11	12 OE 2410135 Problemer med pasientvarsling i Glassblokkene OE2410682 Problemer med nettverk til sentralbord og flere utekontor i Helse Stavanger	13	14
15	16	17	18	19	20	21
22	23 OE 2414839 Utilgjengelighet i LIBRA Produksjon	24	25	26	27	28
29	30 OE 2418814 Feilmeldinger i DIPS Arena					

Kommentarer til hovedrapport:

88% i april

14310 henvendelser før talemelding

12850 henvendelser etter talemelding

4 Omfattende Episoder

12.04.24 Episode 2410135- Problemer med pasientvarsling i Glassblokkene

Incident start: 12.04.24 01:05

Incident løst: 12.04.24 09:39

Nedetid i minutter: 574

Grønn beredskap

Oppsummering av hendelsen:

Problemstillingen i Ascom Regional Plattform /Imatis Mobilportal var forårsaket av sikkerhetsoppdatering (patching) av et databasecluster i løsningen.

Oppdateringen skapte brudd i en tjeneste som gjorde at det ikke kom varsel over fra Ascom til Imatis.
Det finnes for tiden ingen løsninger som vi kan kjøpe fra våre leverandører som løser denne utfordringen, som samtidig benytter SQL infrastrukturtjenesten til HVIKT.
For Ascom Regional Plattform/Imatis Mobilportal måtte alle systemer manuelt restartes.
Det opprettes en arbeidsgruppe som ser mer helhetlig på tjenestene vi leverer i løsningen med tanke på hvilke tiltak som kan og bør gjøres.
Oppfølgning i Problem: P10815
Kundekonsekvens:
Problemer med pasientvarsling i perioden.
Utilgjengelighet i Ascom Regional Plattform/Imatis Mobilportal som berørte sykehusvarsling/ pasientsignal /akuttvarsling og overfall til Imatis på mobil.
Berørte foretak:
Helse Bergen - Glassblokkene
(Alle foretak kan ha blitt berørt i enkelte perioder. HDS, Portørtjeneste og HFO, Overfallstjeneste var berørt i perioder)

12.04.24 2410682 - Problemer med nettverk til sentralbord og flere utekontor i Helse Stavanger
Incident start: 12.04.24 14:05
Incident løst: 12.04.24 20:00 (Jæren og Hå amb.stasjon 13.04.24 18:30)
Nedetid i minutter: 355
Grønn beredskap
Oppsummering av hendelsen:
Sentralbord, samt alle utekontor i Helse Stavanger uten redundant samband, var uten nettverk i deler av perioden.
Feilsituasjonen var forårsaket av at nytt nettverksutstyr ble montert og koblet til strøm i U50A på SUS.
Dette førte til en overbelastning på kurser. Ustabilitet på strømforsyningen førte til en feil i en av ruterne, slik at denne ikke kom opp når strømmen var tilbake/sikringer var resatt.
Rotårsak relatert til at på grunn av en manuell feil/rutinesvikt ble nettverksutstyr koblet til en kurs som ikke nok kapasitet.
Berørte samband er fortsatt uten redundans. Det er bestilt nytt utstyr for å gjenopprette redundans.
Hendelsen gjennomgås for vurdering av ytterligere tiltak.
Oppfølgning i Problem: P10847
Kundekonsekvens:
Sentralbord, samt alle utekontor i Helse Stavanger uten redundant samband, var uten nettverk i deler av perioden.
Berørte foretak:
Helse Stavanger

- Sentralbordet (midl. flyttet ifm. feilsøking av taleproblematikk) OK 15:46
- Øyeblikkelig hjelp Jæren
- Jæren og Hå ambulansestasjon OK 13.04.24 18:30
- DPS Sandnes
- Finnøy ambulansestasjon
- Lagårdsveien 78
- KORUS Stavanger
- LRS i Gartnerveien 4
- Forskningssenter Sandnes
- Lager i Koppholen
- Stavanger ambulansestasjon
- Radiologi Sandnes
- Forus Kjøkken
- Hjelmeland ambulansestasjon
- Barnehuset i Rogaland
- Redundans på andre utekontor hos Helse Stavanger

Jæren DPS
Helse Vest RHF Redundans (ikke utfall, men manglende redundans)

23.04.24: 2414839 Utilgjengelighet i LIBRA Produksjon

Incident start: 23.04.24 06:41

Incident løst: 23.04.24 10:48

Nedetid i minutter: 247

Gul beredskap

Oppsummering av hendelsen:
LIBRA Produksjon/SAP utilgjengelig i perioden. SAP GUI var tilgjengelig og ble brukt av apotekene under hendelsen. Feilsituasjonen var forårsaket av hardwarefeil på en minnebrikke på en av serverene i datahallen som førte til en utilsiktet restart.
Under oppstart av løsningen manglet det routing tabeller.
Dette førte til forlenget nedetid i løsningen. Feilsituasjonen ble løst ved reetablering av rutingtabeller når servere kom opp igjen etter restart.
Minnebrikke med problemer skal byttes ut for å forhindre framtidige feil.
Pågående rotårsaksanalyse i dialog med leverandør.
Oppfølging i Problem: P10856
Kundekonsekvens:
LIBRA Produksjon/SAP utilgjengelig i perioden.
Brukere fikk ikke brukt systemet med normalt grensesnitt Front end (Fiori).
(SAP GUI var tilgjengelig hele tiden (annet grensesnitt).
Alle apotek brukte SAP GUI under hendelsen.
Berørte foretak:

Alle Helseforetak

30.04.24 Episode 2418814 - Feilmeldinger i DIPS Arena

Incident start: 30.04.24 10:40

Incident løst: 30.04.24 15:24

Nedetid i minutter: 0

Grønn beredskap

Oppsummering av hendelsen:

Feilsituasjonen var forårsaket av ressursproblemer på noen av applikasjonsserverne i løsningen.
Dette førte til at ulike applikasjonstjenester i DIPS Arena fikk problemer.
Ressursproblemene var relatert til stor aktivitet med rapportkjøringer.
Rapporttjenesten frigjorde ikke ressurser, og dette skapte problemstillingen.
Løst ved at applikasjonservere med problemer ble tatt ut av løsningen og restartet.
Ny rapporteringsløsning er under etablering. Rapportkjøringen skal flyttes til å gå via Kubernetes og planlegges implementert i neste release (25.05.24).
Tett oppfølging og overvåkning inntil tjenesten er flyttet.
Oppfølging i Problem: P10742

Kundekonsekvenser:

Driftsforstyrrelser og perioder med nedetid i DIPS Arena.
Brukere opplevde forskjellige feilmeldinger og driftsforstyrrelser i perioden.

Berørte foretak:

Alle foretak

Sikkerhetsavvik

Det ble i april 2024 rapportert 80 «mulige sikkerhetsavvik» i Helse Vest IKT sitt sakshåndteringssystem, en nedgang fra mars 2024. En stor andel av disse var tilknyttet automatiserte varsler.

Helse Vest IKT rapporterer sikkerhetssaker i den måneden sakene blir avsluttet/lukket i sakshåndteringssystemet, selv om hendelsene kan være håndtert på et tidligere tidspunkt. De rapporterte «mulige sikkerhetsavvikene» er vurdert/håndtert, og av disse er 49 avsluttet som reelle sikkerhetsavvik.

14 sikkerhetsavvik ble rapportert i avvikssystemet (Synergi eller tilsvarende) til berørte virksomheter for vurdering av om avvikene er reelle.

For samme måned i fjor var tallene 107 mulige sikkerhetsavvik, 71 reelle avvik, hvorav 19 saker ble rapportert i avvikssystem.

De mest frekventerte sikkerhetsavvikene som meldes i Assyst er:

- 25 generelle varsler fra HelseCERT og øvrige kilder vedrørende sårbarheter i produkter og tjenester
- 9 saker gjelder pasientjournalsystemet DIPS
- 8 saker gjelder sårbarheter avdekket i sårbarhetsskanning
- 3 saker gjelder tilgangsstyring på filshare

Følgende saker ble også meldt til foretakenes avvikssystem.

- 8 saker gjelder manglende skjerming av pasient og personopplysninger
- 2 saker vedrører uautorisert bruk av andres bruker-ID og passord
- 4 saker gjelder andre brudd på konfidensialitet
- I april ble 1 sak sendt til helseforetakene som meldepliktig brudd på personvernet. Denne gjaldt brudd på konfidensialitet ved utsending av dokumentet PLO utskrivningsrapport.

Synergisaker ang. IKT-sikkerhet/drift inn til HVIKT:
6 saker ble meldt i april som omhandlet informasjonssikkerhet til Helse Vest IKT i avvikssystemet Synergi. 4 saker ble lukket i samme tidsperiode.

Økonomisk resultat ved utgangen av april

Oversikt
Rapporten for april viser eit drifts- og månadsresultat under budsjett. Resultat hittil i år viser eit underskot på 10,9 mill, og er 16,7 mill under budsjett. Dette skuldast i hovudsak for lite timar levert til investeringsprosjekt. Prognosen er endra til – 5 mill med grunnlag i at det er lite sannsynleg at ein klarer å ta igjen alt underforbruk i leveranse av timar.

Rekneskap per 30.04.2024	Rekneskap	Budsjett	Avvik	Rekneskap Hittil	Budsjett Hittil	Avvik Hittil	Årsbudsjett 2024	Prognose 2024
Basistilskot	5 624	2 931	2 693	13 179	8 794	4 385	35 174	39 174
Andre inntekter	166 804	156 132	10 672	649 603	617 975	31 628	1 859 044	1 909 044
Sum Driftsinntekter	172 428	159 063	13 365	662 782	626 769	36 013	1 894 218	1 948 218
Varekostnadar	-1 778	-2 772	994	-11 759	-11 088	-671	-33 265	-33 265
Lønn- og personalkostnadar	-54 370	-48 617	-5 753	-221 656	-191 451	-30 205	-572 219	-607 219
Øvrige kostnadar	-78 625	-64 299	-14 326	-276 616	-253 696	-22 920	-786 693	-811 693
Av- og Nedskriving	-33 655	-32 863	-792	-132 405	-132 407	2	-404 041	-404 041
Sum Driftskostnad	-168 428	-148 551	-19 877	-642 436	-588 642	-53 794	-1 796 218	-1 856 218
Driftsresultat	4 000	10 512	-6 512	20 346	38 127	-17 781	98 000	92 000
Sum Finans	-7 980	-8 083	103	-31 274	-32 333	1 059	-97 000	-97 000
Totalresultat	-3 980	2 429	-6 409	-10 928	5 794	-16 722	1 000	-5 000

Salsinntekt ligg over budsjett per april. Dette skuldast i hovudsak høgare sal av varer, vidarefakturering av felleskostnadar til andre regionar, samt høgare kostnadar i enkelte områder enn budsjettert.
Lønn- og personalkostnadar har eit avvik mot budsjett på 30,2 mill per april. Dette skuldast i hovudsak:

- mindre timar levert til investeringsprosjekt med 22,3 mill
- mindre refusjonar for sjuke- og foreldrepengar med 0,9 mill
- auka tenestekjøp frå HF'a med 5,9 mill

Øvrige kostnadar har eit avvik mot budsjett på 22,9 mill per april. Dette skuldast i hovudsak:

- kjøp av tele-/signalutstyr med 4,3 mill
- vedlikehald av IKT-infrastruktur med 1,0 mill
- auka kjøp av konsulentar med 6,7 mill
- auka support- og lisenskostnadar løysinger med 10,3 mill

Med eit underskot på 10,9 mill per april er det behov for ekstra innsparingstiltak for å redusere underskot mest mogeleg, og nærme seg årets resultatmål. I styremøte 8. desember vart det vedtatt ein innsparingsplan på 10 mill, og denne følgast opp med dei ulike einingane. I tillegg er det sett på følgande tiltak:

- dialog med områda om moglegheit for auka aktivitet i investeringsprosjekt
- oppfølging av all timeføring
- prioritere leveransar til digitaliseringsprosjekt
- vurdere oppgåvefordeling framfor nytilsetting ved avgang
- vurdere oppgåvefordeling framfor nytilsetting, eller utsetting av rekruttering av nye stillingar

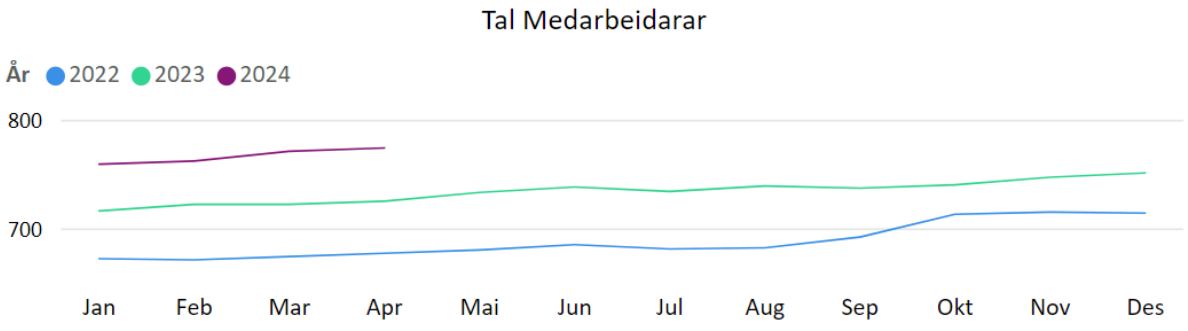
Balanse

Helse Vest IKT har så langt i år tatt opp nytt langsiktig lån frå Helse Vest RHF med 150 mill.

Balanse per 30.04.2024 (tal i 1 000)	2024	2023
Immatrielle eigendelar	1 315 957	1 351 853
Varige driftsmiddel	805 753	728 222
Finansielle anleggsmiddel	8 077	8 077
Sum anleggsmidler	**2 129 787**	**2 088 152**
Varer	36 931	35 603
Krav	505 784	356 407
Bankinnskot	234 459	133 508
Sum omlaupsmidlar	**777 174**	**525 518**
Sum eigendelar	**2 906 961**	**2 613 670**
Aksjekapital	1 000	1 000
Annan innskoten eigenkapital	150 319	150 319
Annan eigenkapital	19 820	30 770
Sum eigenkapital	**171 139**	**182 089**
Pensjonsforplikting	101 198	93 515
Langsiktig gjeld	2 152 618	2 002 618
Kortsiktig gjeld	482 006	335 448
Sum gjeld	**2 735 822**	**2 431 581**
Sum eigenkapital og gjeld	**2 906 961**	**2 613 670**

Personal

Personalressursar

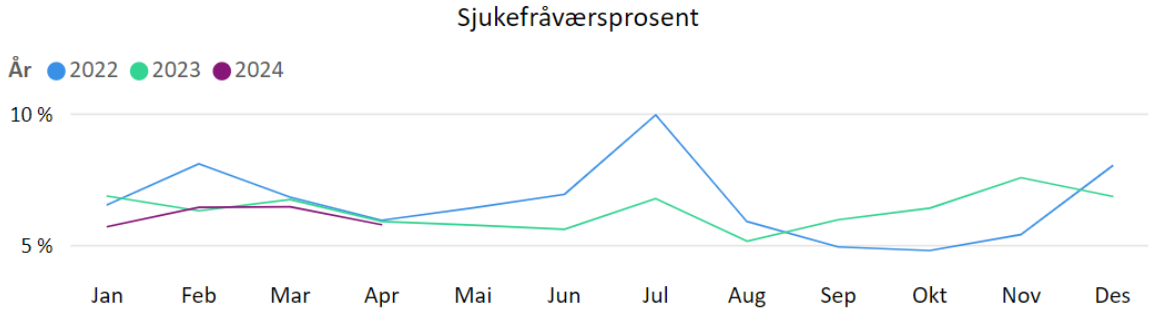


År	Jan	Feb	Mar	Apr	Mai	Jun	Jul	Aug	Sep	Okt	Nov	Des
2024	759	762	771	774								
2023	716	722	722	725	733	738	734	739	737	740	747	751
2022	672	671	674	677	680	685	681	682	692	713	715	714

Snitt hittil i år	Jan	Feb	Mar	Apr
	759	761	764	767

Sjukefråvær

Sjukefråvær i perioden frå mai 2023 til april 2024. Gjennomsnitt siste 12 mnd er på 6,2 %.



År	Jan	Feb	Mar	Apr	Mai	Jun	Jul	Aug	Sep	Okt	Nov	Des
2024	5,7	6,4	6,4	5,8								
2023	6,9	6,3	6,7	5,9	5,7	5,6	6,8	5,1	6,0	6,4	7,6	6,8
2022	6,5	8,1	6,8	5,9	6,4	6,9	9,9	5,9	4,9	4,8	5,4	8,0

Snitt hittil i år	Jan	Feb	Mar	Apr
	5,7	6,0	6,2	6,1

Turnover

Turnover i perioden frå april 2023 til mars 2024. Gjennomsnitt siste 12 mnd er på 6,1 %.

Reel turnover for organisasjon: Alle avdelinger, stillingsgruppe: Alle yrkesgrupper, alder: alle aldre, ansattype: fast

	202401	202402	202403	202404	202305	202306	202307	202308	202309	202310	202311	202312	Snitt siste 12 mnd
Antall sluttet i perioden	2	1	2	2	3	6	8	4	8	2	4	2	44
Tal medarbeidarar	726	733	744	752	702	708	704	706	703	704	715	719	718
Turnover i prosent	**0,28 %**	**0,14 %**	**0,27 %**	**0,27 %**	**0,43 %**	**0,85 %**	**1,14 %**	**0,57 %**	**1,14 %**	**0,28 %**	**0,56 %**	**0,28 %**	**6,13 %**

HELSE VEST IKT AS

SAK 026-24

GÅR TIL:	Styremedlemmer
FØRETAK:	Helse Vest IKT AS
DATO:	06.06.2024
SAKSHANDSAMAR:	Ole Jørgen Kirkeluten, Inger Cathrine Bryne
SAKA GJELD:	**Fornya vurdering av oppseiing Blå Kors**
ARKIVSAK:	
STYRESAK:	**026/24 O**
STYREMØTE:	**13.06.2024**

FORSLAG TIL VEDTAK

1. *Styret tek saka til orientering.*

Oppsummering

Det vises til oppseiing av avtalar om IKT-drift for Blå Kors klinikk Haugaland AS og Rehabilitering Vest AS, samt brev frå Blå Kors der dei ber om ei fornya vurdering av oppseiing av avtalar.
Helse Vest IKT er i dialog med eigaravdelinga i Helse Vest RHF, og RHF'et vil ivareta videre dialog med Blå Kors, samt handtere svar på klagen.

Blå Kors

AKTIV DELTAKELSE OG MESTRING rehabilitering vest

Helse Vest IKT
Att. Styreleder Inger Cathrine Bryne og styrets medlemmer
postmottak@helse-vest-ikt.no

Vår ref: 2024/22 – KANAD/ARVKAM **Deres ref**: **Dato:** 03.05.2024

Fornyet vurdering av oppsigelse

Vi viser til Helse Vest IKTs oppsigelser av våre IT-avtaler. Oppsigelsene har bakgrunn i beslutning fattet av styret i Helse Vest IKT 28.09.2022.

Vi ber om at styret i Helse Vest IKT gjør en fornyet vurdering av disse oppsigelsene idet vi mener beslutningsgrunnlaget for oppsigelsene er mangelfullt, vesentlige momenter ikke er vurdert og konsekvensen for pasientene er negative. Pasientperspektivet var ikke tema i styresaken.

Pasientrelaterte systemer og pasientsikkerhet

Vi benytter og betaler i dag for DIPS Arena og felles bruk av EPJ-løsningen. Våre pasienter er også Helse Vest sine pasienter og å miste tilgangen til DIPS Arena
vil øke faren for feil og/eller mangler når pasienten overføres fra ett ledd til et annet ledd i behandlingskjeden.

Gjennomgående bruk av samme pasientrettede system vil betydelig redusere risikoen for feil knyttet til unøyaktig informasjon om pasientenes tilstand og medisinering.

I nylig avgitt Nasjonal helse- og samhandlingsplan 2024-2027, heter det blant annet:

> *'En stor del av rehabiliteringstilbudet i spesialisthelsetjenesten utføres i private og ideelle rehabiliteringsinstitusjoner som har avtale med de regionale helseforetakene. Regjeringen vil videreutvikle tilbudet gjennom samarbeid mellom store og små sykehus og mellom spesialisthelsetjenesten og kommunene, og ved bruk av digitale løsninger'. (side 32)*

Vi mener at pasienters og helsepersonells behov samt nasjonale målsetninger om sømløse og sammenhengende tjenester på tvers av omsorgsnivå også må være førende for Helse Vest og Helse Vest IKT.

Vi viser til at Helse Vest har pekt ut fem risikoområder de neste områdene som skal følges spesielt opp. Legemiddelhåndtering er ett av dem. Dette er forankret i Helse Vest sin strategi, Helse 2035, Helse Vest sin utviklingsplan og i Regional plan for kvalitet og pasientryggleik 2020- 2024 der det fremgår at Helse Vest arbeider etter å minimere og eliminere feil i forbindelse med legemiddelhåndtering.

Når en pasient under en innleggelse blir overført til en annen virksomhet i Helse Vest, vil det fra 12.03.2024 være mulig å fortsette samme kurve i den virksomheten pasienten overføres til. Med virksomhet menes foretak eller private ideelle (DPI). Dette gjelder hverken for Blå Kors klinikk Haugaland eller Rehabilitering Vest.

Blå Kors

AKTIV DELTAKELSE OG MESTRING rehabilitering vest

IT-sikkerhet

IT-tjenester, spesielt knyttet til spesialisthelsetjenesten stiller meget høye krav til sikkerhet, oppdateringer og løpende oppfølgning for å hindre at data kommer på avveie. Både for virksomhetene og for Helse Vest, som overlater pasienter til institusjonene som en del av sin 'sørge for'-plikt, er det en trygghet i at virksomhetene opererer innenfor Helse Vests egen sikkerhetsinfrastruktur.

Et opphør av eksisterende samarbeid flytter Helse Vest pasientsensitiv informasjon ut av eget IKT-sikkerhetsregime. Vi mener dette bør ha vært risikovurdert før beslutning om slik flytting av pasientsensitiv informasjon gjennomføres.

Økonomiske konsekvenser

Avtalene om kjøp av IT-tjenester skjer etter klare avtaler og på vilkår som sikrer at det ikke foregår subsidiering eller gir andre særskilte fordeler til virksomhetene som kjøper tjenestene.

Våre to virksomheter har for 2024 budsjettert med kjøp av IKT-tjenester fra Helse Vest IKT for til sammen 2,2 millioner kroner.

Avtalene er til minimal belastning for HVIKT. Vi følger kun planlagt drift og oppgraderinger. Vå samlede belastning på kundesenteret tilsvarer beskjedne 1,3 henvendelser daglig. Vi mener at en oppsigelse av oss som kunder tar bort store inntekter og at det kun er minimal besparelse på andre områder, slik at dette vil svekke stordriftsfordelene til HVIKT. Dette kom ikke frem i styresaken.

Modellen med kjøp av IT-tjenester av Helse Vest IKT for samarbeidspartnere som oss med langvarige avtaler med Helse Vest om helsetjenester som en del av Helse Vest 'sørge for'-ansvar er slik sett en modell som bør videreutvikles blant annet for å bidra til oppfylling av målene som settes i nylig avgitt stortingsmelding.

Strukturelle konsekvenser av avvikling

Avtalen med HVIKT gir våre virksomheter storkundefordeler. Dette holder IT-kostnadene i anbudene nede. Dersom HVIKT øker kostnadene for oss gjennom å si opp langvarige avtaler vil det ha som konsekvens at vi må få denne kostnaden kompensert gjennom økte satser fra Helse Vest. Det er ikke ønskelig.

Vi ber styret ha pasientene i fokus og gi administrasjonen i HVIKT fullmakt til å inngå nye avtaler med oss og eventuelt andre aktører som sikrer tilgang til pasientsystemer som Dips Arena og Meona.

Vi ber om at vår klage behandles så raskt som mulig i neste styremøte.

Med vennlig hilsen

Arve Kambe
Direktør, Blå Kors klinikk Haugaland AS

Kari Nådland
Administrerende direktør, Rehabilitering Vest AS

SAK 027-24

GÅR TIL: Styremedlemmer
FØRETAK: Helse Vest IKT AS

DATO: 13.06.2023
SAKSHANDSAMAR: Fredrik Eldøy, Randi Solberg
SAKA GJELD: **Rapportering på bruk av ITIL rammeverk**

ARKIVSAK:
STYRESAK: **Styresak 027/24 O**

STYREMØTE: **13.06.2023**

Innledning

ITIL® er verdens mest brukte IT Service Management-rammeverk. ITIL er en samling av beste praksis, og et verktøy for å optimalisere endring og transformering av IT i en organisasjon. Praksisene danner grunnlaget for å kunne jobbe i tråd med Helse Vest IKTs strategiske mål om å ha en sikker, stabil og effektiv drift av infrastruktur og løysingar. I ITIL rammeverket finnes det 34 globalt anerkjente beste praksiser. Alle de ulike praksisene har grenseflater til hverandre og henger mer eller mindre sammen. Vi har iverksatt 12 av disse og 1 er fortsatt under innføring (Leverandørstyring / Supplier management)

Vi har siden juni 2023 innført 1 ny praksis: Service Level Management som beskriver hvordan vi jobber med SLA/Tjenesteavtalen. I tillegg har vi revidert Service Continuity Management praksisen som beskriver vår beredskapshåndtering og sikring av driften ved driftsforstyrrelser. Nylig har vi også oppdatert endrings-prosessen også kjent som Change Enablement Management.

Status for ITIL rammeverk i Helse Vest IKT

I tidligere styresaker om ITIL praksisene har vi rapportert på etterlevelse av praksiser som er iverksatt i tillegg til en modenhetsevaluering pr praksis. I denne styresaken har vi valgt å vektlegge hvordan praksisene brukes i Helse Vest IKT og hvordan de skaper verdi.

Vi ønsker å gi styret en overordnet status fra seksjon Prosess og forbedring som nå er ansvarlig for ITIL praksisene i Helse Vest IKT.

De 12 innførte ITIL praksisene har alle en kobling til Helse Vest IKT sine 4 strategiske mål. Praksisene sikter særlig på målet om å ha en sikker, stabil og effektiv drift av infrastruktur og løysingar.

Fokuset vårt i utviklingen av praksisene er å tilrettelegge for verdiskapning samtidig som vi ivaretar kvalitet, risiko og kosteffektivitet i tjenestene. Praksisene skal være i tråd med relevante Objectives and Key Results (OKRs) for Helse Vest IKT.

Ny styringsstruktur og nye former for samhandling krever at ITIL praksisene holder tritt med utviklingen av organisasjonen. Standardisering og kontinuerlig forbedring av arbeidsmetoder er blitt enda viktigere når vi skal redusere tid fra behov til levert nytteverdi. Når endringstakten økes, må vi fortsatt ha tilstrekkelig med styring og kontroll. Praksisbeskrivelsene skal fremme standardiserte måter å arbeide på. Dette skal gjøre det enklere for team å samhandle med hverandre. Det er her ITIL praksisene kommer til sin rett. Når det skal gå fort er det ikke tid til å lure på hvordan man skal jobbe eller samhandle.

Når farten øker, vil vi få flere endringer og flere produksjonssettinger. Dette har vi etablerte praksiser for. Når disse etterleves øker vi sjansen for at endringer og produksjonssettinger gjøres uten uønskede driftsforstyrrelser.

Under er en overordnet oppsummering av aktiviteter som gjennomført siden juni 2023 og områder vi kommer til å sette søkelys på i tiden fremover.

Overordnet status på praksisene:

Incident Management (Episode) Praksisen har fått ny rapportering med etablering av Driftskalender. Ny Driftskalender gir raskt overblikk over driftsstabilitet i rapporter. Metodikk for gjennomgang av Omfattende Episoder er oppdatert og danner grunnlag for å finne og jobbe med læringspunkter etter driftsforstyrrelser. Disse læringspunktene følges opp med tiltak. De følges opp av praksisen Problem Management.

Sikkerhets Operasjons Senter (SOC) ble etablert april 2024 for å oppdage og håndtere sikkerhets-incidents.

Problem Management: Vi har løst og avsluttet 146 problemsaker siste 12 måneder. Det er for eksempel blitt rettet feil som har hatt risiko for pasientsikkerhet og det har vært gjort tiltak for å øke ytelse i de store kliniske systemene. Over halvparten av alle åpne problemsaker (617) ligger hos våre underleverandører. Problem Management kobles mot OKR som handler om å redusere plunder og heft. Dette skaper verdi ved å frigi tid og hender i sykehusene.

Change enablement Management – Den gamle endringsprosessen er blitt revidert. Change Enablement praksisene er koblet mot OKR der målet er at antall endringer skal opp samtidig som uønskede driftsforstyrrelser etter endringer skal ned. Det holdes ukentlige møter (Endringsråd og Beslutningsråd) for å vurdere risiko og egnet tidspunkt for endringer som driftsorganisasjonen må være særlig oppmerksomme på. På intranett ligger det en endringskalender som viser alle godkjente/planlagte endringer. På en tilfeldig uke i mai var det forhåndsmeldt 48 endringer.

Release Management: Den beste måten å innføre nye systemer og løsninger på er å følge denne praksisen. Det finnes sjekklister og velprøvde metoder for sikker og god produksjonssetting. Når praksisen følges er Kundesenteret påkledd når brukeren ringer inn og trenger hjelp.

Service Configuration Management (Konfigurasjon) **-** Det pågår kontinuerlig arbeid med å holde oversikt over systemer, konfigurasjonsenheter og sammenhengen mellom. Hovedverktøyet for vår konfigurasjonsbase (CMDB) er assyst. Det har kommet en bestilling fra Sikkerhetsleder Helse Vest som heter: Hvordan oppnå effektiv oversikt over utstyr, enheter og programvare på tvers av IKT miljøer i Helse Vest. Dette arbeidet er viktig for å øke sikkerheten i det totale IKT-miljøet.

Knowledge Management I Helse Vest IKT er kunnskap dokumentert på sharepointsider, i teamskanaler, og i ulike system. Hovedkilden for Kundesenteret er assyst der kunnskapsartikler kan søkes opp mens man forsøker å løse en Inicdent eller service-request. Når kunnskapsartiklene er oppdaterte og søkbare redusere dette tiden det tar å få løst brukernes henvendelser.

Service Request Management (Standard leveranser): Vi opplever stor suksess med Kundeweb / selvbetjeningsløsninger. Brukere får raskere hjelp og slipper å ringe for å melde behov. Vi har snart like mange kundeweb-meldinger som telefoner til Kundesenteret, typisk 500 av hver pr dag.

Tilganger er en type Service Requests. På en gjennomsnittlig måned høsten 2023 håndterte Samlepunktet 12.500 tilgangsbestillinger og 2500 passord-resettinger. Det meste av tilgangshåndtering er automatisert.

Service Level Management (SLA/Tjenesteavtalen). Ny praksis. Hvordan vi jobber sammen med helseforetakene for å holde tjenesteavtalen oppdatert er dokumentert og kvalitetssikret mot beste praksis. Tjenesteavtalen oppdateres nå fortløpende og ikke en gang i året som tidligere.

Service Continuity Management: Praksisen er revidert, gjort kjent og tydeliggjort. Praksisen danner grunnlaget for det videre arbeidet med delplaner for beredskap innen IKT og forsyning. Praksisen inneholder også maler for å utarbeide beredskapsplaner for sentral infrastruktur og løsninger. Praksisen setter krav om beredskapsøvelser på ulike nivåer.

Information Security Management: Formålet med praksisen er å sikre at informasjon blir beskyttet mot en rekke trusler for å sikre kontinuitet i virksomheten. De tre søylene som praksisen bygger på er integritet, konfidensialitet og tilgjengelighet.
Praksisen rapporter blant annet på oppdagede sikkerhetsavvik.

Service Validation & Testing Management: Det lages nå et rammeverk for gjennomføring av sikkerhets- og User-eXperience / Universiell Utforming -testing (UX/UU). Implementering av testautomatisering. Se på testprosessen opp mot ny områdestruktur – identifisering og implementering av beste praksis.

Monitoring and event Management: Helse Vest IKT har et eget team som bygger og vedlikeholder overvåkingsløsninger. Det handler om å finne et systems normaltilstand og når tilstanden til et system avviker så mye at det må reageres. Driftsvakten oppdager og fikser jevnlig små og store feil før brukerene merker noe.. For eksempel: Tidligere hadde vi driftsforstyrrelser som skyldtes fulle disker og sertifikater som gikk ut på dato. Det har vi lite av nå.

Satsingsområder for neste periode frem til juni 2025:

Oppfølging! Service Continuity Management: Beredskap, beredskapsøvelser og beredskapsplaner er blitt høy aktualisert grunnet den sikkerhetspolitiske situasjonen i Europa. Beredskapsplaner for kritisk viktige systemer og infrastruktur kan bli bedre.

Ny! Servicedesk Management. Kundesenteret drives i dag etter beste praksis men det gjenstår å dokumentere praksisen. Dette er en såkalt lavt hengende frukt.

Forslag til vedtak:

1. Styret tek saka til orientering.

HELSE VEST IKT AS

SAK 028-24

GÅR TIL:	Styremedlemmer
FØRETAK:	Helse Vest IKT AS
DATO:	06.06.2024
SAKSHANDSAMAR:	Ole Jørgen Kirkeluten
SAKA GJELD:	**Innkalling til ordinær generalforsamling i Helse Vest IKT AS**
ARKIVSAK:	
STYRESAK:	**028/24 B**
STYREMØTE:	**13.06.2024**

FORSLAG TIL VEDTAK

1. *Styret kallar inn til ordinær generalforsamling i Helse Vest IKT AS i tråd med innkalling og vedlegg.*

Oppsummering

Viser til sak 006/24 om godkjenning av styret sin årsberetning for 2023, godkjenning av årsrekneskap for 2023, og godkjenning av rapport for leiarløn og anna godtgjersle for 2023.

Viser til aksjelova vedrørande ordinær generalforsamling.

Forslag til innkalling og vedlegg til generalforsamling er lagt ved i vedlegg 1 (vedlegg 1 til sak 028/24, årsrekneskap med styret sin årsberetning og revisjonsberetning, samt rapport om løn og anna godtgjersle er ikkje sendt ut som eige vedlegg).

HELSE VEST IKT AS

INNKALLING TIL ORDINÆR GENERALFORSAMLING
HELSE VEST IKT AS

GÅR TIL:	Generalforsamling Styreleiar Agnes Landstad, Helse Vest RHF
FØRETAK:	Helse Vest IKT AS
DATO:	Fredag 14.06.2024, kl 08:30 – 09:00
SAKSHANDSAMAR:	Ole Jørgen Kirkeluten
SAKA GJELD:	**Innkalling til ordinær generalforsamling i Helse Vest IKT AS**

Sakliste

Opne saker

Sak 001/24	Val av møteleiar
Sak 002/24	Godkjenning av innkalling/dagsorden
Sak 003/24	Val av representant til å underskrive protokollen saman med møteleiar
Sak 004/24	Godkjenning av årsrekneskap, styret sin årsberetning og rapport for løn og godtgjersle for Helse Vest IKT for 2023 (vedlegg)
Sak 005/24	Val av styremedlemmer (vedlegg)
Sak 006/24	Fastsetjing av honorar til styremedlem (vedlegg)
Sak 007/24	Fastsetjing av honorar til revisor (vedlegg)

Bergen, 06.06.2024
Helse Vest IKT AS

Inger Cathrine Bryne
styreleiar

HELSE VEST IKT AS

SAK 029-24

GÅR TIL:	Styremedlemmer
FØRETAK:	Helse Vest IKT AS
DATO:	06.06.2024
SAKSHANDSAMAR:	Ole Jørgen Kirkeluten, Aksel Bruun, Knut Gjærde
SAKA GJELD:	**Trusselvurdering for spesialisthelsetenesta 2024**
ARKIVSAK:	
STYRESAK:	**029/24 O**
STYREMØTE:	**13.06.2024**

FORSLAG TIL VEDTAK

1. *Styret tek saka til orientering.*

Oppsummering

Ei vellukka cyberangrep mot spesialisthelsetenesta kan føre med seg store konsekvensar for spesialisthelsetenesta si evne til å utføre sine primæroppgåver. Dagens trusselbilete er komplisert og i konstant endring som følgje av trusselaktørane si auka evne til tilpassing og utvikling av verktøy og metodar.

Kriminelle aktørar er framleis den største trusselen, spesielt digital utpressing som kan føre til høg skade. Statlege aktørar frå Russland og Kina utgjer også betydelege truslar med høg evne til cyberspionasje.

Verda er inne i ein periode med geopolitisk ustabilitet, mellom anna som følgje av krigen i Ukraina og Gaza. Dette påverkar alle trusselaktørar, og vil kunne endre prioritering om målutveljing raskt. Som følgje av trusselbiletet mot spesialisthelsetenesta er det derfor avgjerande å jobbe i fleire dimensjonar innanfor cybersikkerheitsområdet.

Trusselvurdering 2024

Det digitale trusselbildet mot spesialisthelsetjenesten

HELSE MIDT-NORGE HELSE NORD HELSE SØR-ØST HELSE VEST Norsk helsenett Helse- og KommuneCERT

Sammendrag

Trusselvurdering 2024

Et vellykket cyberangrep mot spesialisthelsetjenesten kan medføre store konsekvenser for spesialisthelsetjenestens evne til å utføre sine primæroppgaver. Dagens trusselbilde er komplisert og i konstant endring som følge av trusselaktørenes økte tilpasningsevne og utvikling av verktøy og metoder.

Vi vurderer at den mest alvorlige trusselen mot spesialisthelsetjenesten fortsatt er kriminelle aktører, og da særlig digital utpressing. Skadepotensialet av et slikt angrep kan være **meget høy**, og kan innebære både nedetid på tjenester, høye kostnader for opprydding og gjenopprettingstid. Evnen organisert kriminelle har til å gjennomføre cyberangrep er **høy**, og de investerer både tid og penger i å videreutvikle sine metoder. De gjennomfører sofistikerte angrep på tvers av sektorer. Målutvelgelsen er opportunistisk, samtidig er det tegn på en mer strategisk målutvelgelse basert på mengden verdifull informasjon. Organiserte kriminelle sin vilje til å utøve angrep mot spesialisthelsetjenesten er **meget høy**, og det er liten risiko for å bli identifisert og straffeforfulgt.

Statlige aktørers vilje til å utøve spionasje utgjør en betydelig trussel mot spesialisthelsetjenesten. Russland har mistet flere diplomater etter invasjonen av Ukraina, og deres tilgang til informasjon om norske interesser er svekket. Russlands vilje til å gjennomføre cyberspionasje mot spesialisthelsetjenesten vurderes til å være **høy**. Kinas vilje vurderes også til å være **høy**, med hensikt å styrke økonomi og posisjon i verdensbildet. Både Russland og Kina har **meget høy** evne til å gjennomføre cyberspionasje uten at dette oppdages. Skadepotensialet knyttet til cyberspionasje er **høyt**, og kan true nasjonale sikkerhetsinteresser.

Hacktivisters vilje til å ramme spesialisthelsetjenesten har gått ned fra i fjor, og vurderes i år til **medium**. Det er viktig å være bevisst på at viljen til hacktivistgrupper kan endre seg raskt med bakgrunn i skiftende geopolitisk situasjonsbilde, betente mediesaker eller andre saker som kan fange hacktivisters oppmerksomhet. Vi ser en klar sammenheng mellom mediesaker og hvordan det fremprovoserer prioriterte mål. Felles for disse er at jo mer oppmerksomhet sakene får i internasjonale og russiske medier, desto mer sannsynlig er det at hacktivister bruker sakene som et påskudd for å gjennomføre angrep. Vi vurderer det som **meget sannsynlig** at skadepotensialet for tjenestenektangrep til å være lavt og kortvarig. Sammenlignet med de andre aktørgruppene vurderes evnenivået til hacktivister som **lav**.

Det vurderes som **meget sannsynlig** at spesialisthelsetjenesten vil oppleve uønskede hendelser som følge av innsidevirksomhet, men at skadepotensialet vil kunne variere fra **ubetydelig** til **meget høyt**. Skadepotensialet fra en innsider vil variere basert på evne og vilje til å skade virksomheten. Dette avhenger av rettighetsnivå, teknisk kunnskap og myndighet.

For å motstå avanserte cyberangrep kreves det en helhetlig tilnærming til sikkerhetsarbeidet. Man må sikre at man har gode grunnleggende sikkerhetsbarrierer som stopper opportunistiske angrepsforsøk for å senke risiko for vellykkede angrep. Spesialisthelsetjenesten kan også tiltrekke oppmerksomhet fra svært avanserte statlige trusselaktører, som kan omgå grunnleggende sikkerhetsbarrierer. Dette betyr at spesialisthelsetjenesten må ha velutviklede metoder for å avdekke uønsket aktivitet og for å igangsette nødvendige tiltak.

Verden er inne i en periode med geopolitisk ustabilitet, blant annet som følge av krigen i Ukraina og Gaza. Dette påvirker samtlige trusselaktører og vil kunne endre prioritering om målutvelgelse raskt. Som følge av trusselbildet mot spesialisthelsetjenesten er det derfor avgjørende å jobbe i flere dimensjoner innenfor cybersikkerhetsområdet.

Innhold

	Hvordan lese rapporten	s.4
Kapittel 1	Oversikt over trusselaktører som er mest relevant for spesialisthelsetjenesten	s.6
Kapittel 2	Organiserte kriminelle aktører	s.8
Kapittel 3	Statlige trusselaktører	s.11
Kapittel 4	Hacktivister	s.19
Kapittel 5	Innsidere	s.21
Kapittel 6	Cybersikkerhetsutfordringer	s.24
	Referanseliste	s.26

Forsidebilde: Shutterstock | Grafisk design: Gnist Design

Hvordan lese rapporten

Sannsynlighetsord
I trusselvurderingskapitlet er vurderingene plassert på slutten av hvert delkapittel for tydelig å skille egne vurderinger fra informasjon hentet fra andres kilder. Kildereferanser er viktige for integritet, sporbarhet og annerkjennelse av andres arbeid. I denne rapporten brukes tall i parentes i teksten, for eksempel [99]. Referansene finner man igjen i kildelisten bakerst i rapporten. I våre vurderinger er det nødvendig at begrepsbruken er konsekvent. Derfor benyttes sannsynlighetsordene listet i tabellen til høyre.

Oversikt over trusselnivåer
Nivåene i tabellen til høyre brukes for å gjøre en overordnet totalvurdering av trusselaktørenes vilje og evne, og en grov vurdering av skadepotensial for spesialisthelsetjenesten. Skadepotensialet er avhengig av mange faktorer og er svært vanskelig å forutsi. Vi ønsker likevel å gi leseren en indikasjon på skadepotensialet av et angrep fra de ulike aktørene. Vurderingen av dette er basert på åpne kilder og er ikke knyttet til eget sårbarhetsnivå. Evnenivået er basert på aktørenes ressurser med hovedvekt på cyberkapabiliteter. Hensikten med tabellen er å kunne gi leser en god oversikt og gjøre det enklere å sammenligne aktørene. Det presiseres at teksten i vurderingene bør vektlegges mer enn tabellene.

Konfidensnivå
Rapporten er i hovedsak basert på pålitelige kilder og resultatene presenteres derfor generelt med et høyt konfidensnivå. Dersom enkelte av vurderingene er usikre eller basert på et tynt kildegrunnlag, er vurderingsordet markert med * for medium konfidensnivå eller ** for lavt konfidensnivå.

Avgrensninger
Tradisjonell etterretningsprossess ligger til grunn for utarbeidelsen av denne rapporten. Trusselvurderingen er utarbeidet for spesialisthelsetjenesten og er produsert ved å analysere, sammenstille og vurdere sentrale åpne rapporter og interne kilder. De nasjonale trussel- og risikovurderingene fra Politiets sikkerhetstjeneste (PST) [1], Etterretningstjenesten (ETJ) [2] og Nasjonal Sikkerhetsmyndighet (NSM) [3] er vektlagt tyngst.

Trusselvurderingen skal ta for seg de mest relevante typene trusselaktører og deres evne og vilje til negativt å påvirke spesialisthelsetjenestens verdier, primært gjennom digitale operasjoner og verktøy. Terrorisme i tradisjonell form er et eksempel på en trussel som ikke dekkes i vurderingen. Videre dekkes ikke utilsiktede hendelser, som for eksempel naturkatastrofer og strømbrudd. Kildegrunnlaget til denne vurderingen er basert på observerte og rapporterte hendelser. Dette er en avgrensning man må være oppmerksom på, da det er mye trusselaktivitet som aldri blir fanget opp.

Vurderingene er basert på informasjon innhentet frem til 22. april 2024 og må forstås deretter. Tidsperspektivet for vurderingene er ett år fra rapporten publiseres.

Sannsynlighetsord	Forklaring	Prosent
Meget sannsynlig	Det er meget god grunn til å forvente	>90%
Sannsynlig	Det er grunn til å forvente	60-90%
Mulig (like sannsynlig som usannsynlig)	Det er like sannsynlig som usannsynlig	40-60%
Lite sannsynlig	Det er lite grunn til å forvente	10-40%
Meget lite sannsynlig	Det er svært liten grunn til å forvente	<10%

Vilje	Evne	Skadepotensiale
Meget høy	Meget høy	Meget høyt
Høy	Høy	Høyt
Medium	Medium	Medium
Lav	Lav	Lavt
Meget lav	Meget lav	Meget lavt

Konfidensnivå	
Høy	(Ingen merknad, hele rapporten)
Medium	*
Lav	**

Foto: Luis Villasmil, Unsplash

Kapittel 1

Oversikt over trusselaktører som er mest relevant for spesialisthelsetjenesten

Trusselvurderingen skal beskrive trusselbildet mot spesialisthelsetjenesten fra relevante trusselaktører. For å beskrive trusselbildet mot spesialisthelsetjenesten på en helhetlig måte, er trusselaktørene gruppert etter en kombinasjon av organisering og intensjon.

Trusselvurderingen er delt inn etter denne grupperingen, men skillet mellom disse blir stadig mer utydelige. Dette skyldes økt samarbeid mellom aktørene. Det er utfordrende for virksomheter å attribuere hvilken aktør som står bak et angrep.

For eksempel kan det være flere aktører inne i et system under et cyberangrep, som gjerne bruker samme skadevare og har stort overlapp i metoder og verktøy. I tillegg er det flere som peker på ulike former for samarbeid og grader av knytninger mellom statlige aktører, organiserte kriminelle aktører og hacktivister [4] [5] [6] [7].

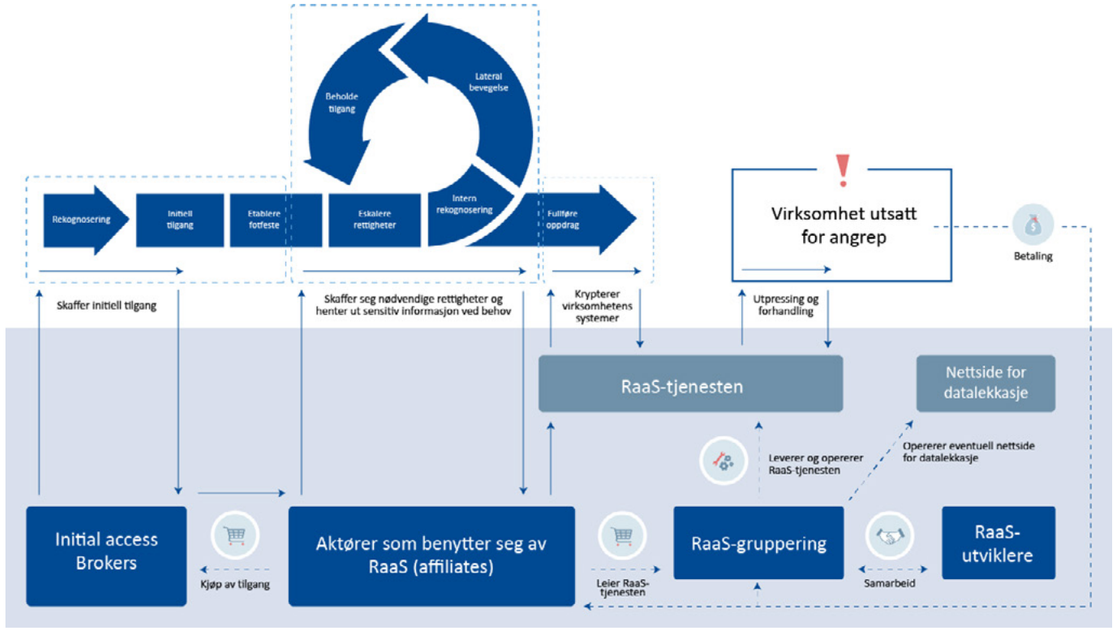
- **Organiserte kriminelle aktører**
  I denne rapport anses de som aktører som opererer ulovlig i cyberdomenet, og er hovedsakelig drevet av økonomisk vinning. Et eksempel på slike aktører er de som driver med digital utpressing.

- **Statlige aktører**
  Statlige aktører defineres her som andre staters etterretnings- og sikkerhetstjenester, inkludert aktører engasjert av disse. Statlige aktører utfører blant annet etterretningsoperasjoner i cyberdomenet.

- **Hacktivister**
  Hacktivister kan være enkeltpersoner eller grupper, og utfører digitale angrep for å formidle politiske eller ideologiske budskap.

- **Innsidere**
  Innsidere defineres som en person som har eller har hatt legitim tilgang til virksomhetenes systemer eller verdier, og som misbruker tilgangen for å skade virksomheten. Innsideaktivitet kan gjennomføres på egenhånd, eller på vegne av en statlig aktør, kriminelle, andre enkeltindivider eller for egen vinning. Fellesnevneren er at innsideren har kapasitet, intensjon og mulighet til å utføre uønskede handlinger.

Foto: Shutterstock



Figur 4: RaaS-økosystem, modellen er inspirert av Microsoft [22].

Kapittel 2

Organiserte kriminelle aktører

Aktørlandskapet knyttet til organiserte kriminelle aktører er et komplekst økosystem som består av flere undergrupper av aktører [8], og det er vanskeligere å skille grupperinger fra hverandre. Årets trusselvurdering vil derfor vurdere organiserte kriminelle aktører som helhet.

Felles for grupperingene innenfor organiserte kriminelle er at de primært drives av økonomisk vinning. Aktørenes økonomiske motivasjon er høy, og de er velorganiserte. De organiserte kriminelle aktørene samarbeider på tvers av landegrenser og innenfor økosystemet av kriminelle. Aktørene lærer av angrepene de gjennomfører, og forbedrer kontinuerlig sine verktøy, teknikker og modus operandi. Dette øker aktørenes kapabiliteter og robusthet, fordi de blant annet har mulighet til å spesialisere seg og effektivisere angrepene [9] [10].

Innenfor økosystemet av kriminelle finnes det ulike grupperinger. En viktig gruppering er Ransomware-as-a-Service (RaaS)-aktørene som stiller med skadevare som krypterer virksomhetens systemer, i tillegg til kommunikasjons- og betalingsløsninger. Tjenestene de tilbyr leies ut til andre aktører for en andel av fortjenesten i angrepet, ofte 10-20 % [11].

RaaS-modellen er utviklet som en forretningsmodell som gjør at RaaS-aktørene kan skalere raskt og øke inntjening. Samtidig kan de operere med lav risiko for å bli tatt, fordi aktørene bak RaaS eksponerer seg ikke i nettet til virksomheter.

Trusselaktørene som benytter RaaS kalles affiliates i RaaS-modellen (se figur på neste side). Det er affiliates som gjennomfører angrep hos virksomheter og kjører krypteringsskadevaren som de leier av en RaaS-aktør [11].

Organiserte kriminelle aktørers utvikling

Global statistikk viser at angrep mot helsesektoren har økt noe, sett opp mot fjoråret. Trusler knyttet til cyberspionasje og cyberkriminalitet anses mest fremtredende for helsesektoren [11] [12]. De fleste angrepene som er gjennomført av organiserte kriminelle er opportunistisk og finansielt motivert, men de siste to årene er det observert aktivitet som tyder på større grad av kartlegging og målrettethet [13] [14].

Organiserte kriminelle aktører peker i større grad ut virksomheter som mulig mål basert på sårbarheter eller endringer [15] [14] [16]. En stor del av organiserte kriminelle aktører utfører opportunistiske kampanjer. Disse refereres gjerne til som *"Big Game Hunting (BGH)"*. Hensikten er å oppnå tilgang til systemer eller finne sårbarheter som kan utnyttes. BGH benytter mer strategisk målutvelgelse av ofrene, og de går gjerne etter virksomheter som har sensitiv og verdifull informasjon [17] [14] [4] [18]. Disse aktørene velger sine ofre basert på deres mulighet til å betale løsepenger, og sannsynligheten for at de vil betale. Helseinstitusjoner trekkes frem som aktuelle ofre, blant annet som følge av at nedetid kan ha kritiske konsekvenser [18].

Organiserte kriminelle og den geopolitiske situasjonens påvirkning

Verden er inne i en periode med geopolitisk ustabilitet, blant annet som følge av krigen i Ukraina og Gaza. Dette påvirker ulike grupperinger innenfor organiserte kriminelle aktører. Etter invasjonen av Ukraina har spesielt russiskbaserte organiserte kriminelle opplevd forstyrrelser i sitt økosystem [19]. Endringer i den geopolitiske situasjonen kan være spesielt interessant for aktører som spesialiserer seg på videresalg av informasjon. Verdien av informasjon kan endre seg som følge av geopolitiske endringer [20], noe som kan påvirke målutvelgelsen til trusselaktørene. De endrer gjerne strategi og taktikk basert på situasjonen for å oppnå profitt.

Organiserte kriminelles aktørers vilje

Organiserte kriminelle aktører har primært økonomisk vinning som formål, og derfor er også deres angrep mindre målrettet. Motivasjonen for å utføre angrep på helsesektoren er hovedsakelig opportunistisk. Metodene aktørene benytter varierer, blant annet ved bruk av skadevare, phishing og sosial manipulasjon.

Enkelte aktører henter ut sensitiv informasjon fra virksomheter for å selge det videre, for eksempel i forbindelse med industrispionasje. Andre ganger kan målet være å få tak i påloggingsopplysninger, enten for direkte salg eller som et steg i å få tak i informasjon som kan selges [15] [20] [21] [22].

Gjennom det siste året har det vært en økning i salg av kompromitterte tilganger med 20 %, og det er stor spredning i geografi og sektorer som rammes [23]. Salg skjer hovedsakelig til andre organiserte kriminelle, samtidig som det i økende grad også selges til statlige aktører. Fremover forventes det at de organiserte kriminelle aktørene som selger kompromitterte tilganger og utvikler skadevaren, fortsetter å knytte tettere bånd [9] [21] [4].

En annen metode aktørene benytter, er å ta kontroll over informasjon eller systemer til en virksomhet og gjøre de utilgjengelig ved bruk av skadevare som krypterer systemene. Globalt har et større antall helseinstitusjoner og sykehus vært offer for utpressingsangrep, der løsepengesummen har vært av en betydelig størrelse i antall angrep med bruk av utpressingsskadevare [12] [11] [4].

Aktørene som benytter utpressingsskadevare som metode har også tatt i bruk det som omtales som dobbel utpressing. Her henter aktørene ut sensitiv informasjon fra offerets systemer, for eksempel helseopplysninger. Deretter krever aktøren løsepenger fra virksomheten for å ikke offentliggjøre eller videreselge disse opplysningene [11] [21].

Organiserte kriminelle aktørers evne
Fremgangsmåtene til aktørene er i kontinuerlig utvikling. I løpet av den siste perioden har man sett en økende trend i å benytte kunstig intelligens (KI). KI benyttes både for å gjennomføre mer sofistikert phishingangrep, og til å utvikle mer avansert skadevare [1] [28]. Aktørene spesialiserer seg også innenfor sektorer og systemer, og er ofte bare en del av et større bilde [15] [24] [25]. Aktørene lærer og utvikler metodene sine fra angrepene de gjennomfører. I tillegg samarbeider de med andre grupper innenfor økosystemet av organiserte kriminelle [21] [15].

Siden flere av aktørene ikke utfører fullverdige angrep selv, er det lavere risiko for å bli oppdaget og straffeforfulgt. Samtidig bidrar de sterkt til profesjonelle cyberangrep gjennom spesialiseringer, som for eksempel salg av tilganger som andre aktører benytter [8] [10].

Metoden som oftest benyttes av cyberkriminelle er utpressingsskadevare, og denne trenden er økende. Evnen og kapabilitetene til disse aktørene er under kontinuerlig utvikling, som følge av at ny teknologi og nye fremgangsmetoder blir tilgjengelige. Samtidig viser utviklingen en økning knyttet til utpressing istedenfor kryptering av virksomheters informasjon og data [4] [16].

Det forventes at sosial manipulering fremover blir mer sofistikert, der metoder som fakturasvindel og direktørbedrageri fortsetter [4]. Antall angrep mot bedrifter og organisasjoner ble redusert i 2023 sett opp imot 2022. Det gjennomsnittlige utbyttet økte derimot til nær det dobbelte. En av utfordringene med tallgrunnlaget på dette området er at det mest sannsynlig er store mørketall grunnet underrapportering [24]. Det er observert flere forsøk på direktørbedrageri innenfor helsesektoren, og dette er en trussel som forblir aktuell.

Vurdering:

Organiserte kriminelle aktører

Overordnet vurdering mot spesialisthelsetjenesten: Organiserte kriminelle aktører			
	Vilje	**Evne**	**Skadepotensiale**
Organiserte kriminelle aktører	Meget høy	Høy	Meget høyt

Vi vurderer at den mest alvorlige trusselen mot spesialisthelsetjenesten er organiserte kriminelle aktører. Organiserte kriminelle aktører er opportunistiske i sin målutvelgelse. Motivet er økonomisk vinning, og aktørenes vilje er **meget høy**. Dette er begrunnet i økt antall angrep globalt, inkludert mot helsesektoren. Aktørene har stor spredning i valg av mål og fremgangsmåter, både med hensyn til land og sektor, men det er fortsatt hovedsakelig opportunistisk utvelgelse. Samtidig er det økende samarbeid mellom aktørene og noe mer strategisk målutvelgelse basert på sensitiv og verdifull informasjon.

Aktørenes evne er **høy**, da de er profesjonelle og tilpasningsdyktige med høy motivasjon for inntjening. Profesjonaliteten fortsetter å øke, og vi ser at aktørene stadig forbedrer sine teknikker. Verktøyene aktørene benytter er blitt betydelig kraftigere og lettere tilgjengelig. Angrepsmetodene er sofistikerte, og trusselaktørene bruker god tid på å gjennomføre angrep. Videre bruker de avanserte metoder for å skjule sin aktivitet. Summen av dette har gjort at suksessraten på angrepene er høyere, noe som medfører økt sannsynlighet for kompromittering. Aktørene har også lav risiko for å bli straffeforfulgt.

Skadepotensialet som følge av angrep fra organiserte kriminelle er vurdert til **meget høyt**, basert på hendelser i sammenlignbare virksomheter globalt. Et angrep som tar ut kritiske systemer kan ramme elektiv og akutt pasientbehandling på kort og lang sikt, og medfører høye kostnader i gjenopprettelse. I tillegg kan kompromittering og publisering av person- og helseopplysninger kunne skade spesialisthelsetjenestens tillit hos befolkningen.

Det gjennomføres kontinuerlig forsøk på angrep mot spesialisthelsetjenesten, og vi vurderer det som **meget sannsynlig** at spesialisthelsetjenesten vil utsettes for cyberangrep gjennomført av organiserte kriminelle aktører. Aktørenes vilje er **høy**, og det er verdifull informasjon som kan omsettes til økonomisk vinning, både gjennom videresalg og utpressing. I tillegg vil nedetid på kritiske systemer kunne medføre alvorlige konsekvenser. Utvikling i den geopolitiske situasjonen vil også kunne påvirke målutvelgelse for organiserte kriminelle aktører, og spesialisthelsetjenesten vil kunne bli et mer attraktivt mål.

Foto: Shutterstock

Kapittel 3

Statlige trusselaktører

I trusselvurderingene fra etterretnings- og sikkerhetstjenestene (EOS-tjenestene) beskrives Russland som den største etterretningstrusselen mot Norge i 2024, og trusselen fra Kina er framhevet som økende [2]. Cyberoperasjoner er den foretrukne metoden brukt av fremmede etterretningstjenester for å gjennomføre spionasje, påvirkning og destruktive cyberangrep. Cyberoperasjoner er kostnadseffektiv og kan ramme et større antall mål med lav risiko for oppdagelse [26] [22] [1] [12] [3].

Spesialisthelsetjenesten forvalter betydelig mengde informasjon som har verdi for statlige trusselaktører, dette gjør oss utsatt for cyberangrep i årene fremover. EOS-tjenestene trekker frem Russland og Kina som de som står bak de mest avanserte operasjonene mot norske virksomheter. Russland og Kina har styrket det strategiske samarbeidet, der de har en sammenfallende interesse i å svekke Vesten [17] [27] [28] [22] [3].

3.1 Cyberspionasje

Cyberspionasje er spionasje eller etterretningsoperasjoner i cyberdomenet gjennomført av statlige trusselaktører. Enkelte land gjennomfører cyberspionasje av politiske grunner, for å oppnå økonomisk vinning eller for konkurransefortrinn. Utviklingen i cyberdomenet fører til at denne typen etterretningsvirksomhet kan gjennomføres i mye større skala enn tidligere. Cyberspionasje er i utgangspunktet tyveri av sensitiv informasjon, uten at motparten forstår at informasjonen er på avveie. Dette kan omfatte både selve informasjonen og systemene, hvor denne informasjonen ligger lagret, som er kompromittert. Derfor er det viktig for trusselaktøren at den tekniske gjennomføringen ikke medfører forstyrrelser på målet og at aktiviteten ikke blir oppdaget [14] [35] [26] [1].

Spesialisthelsetjenesten er en grunnleggende tjenestene i samfunnet og har en viktig beredskapsfunksjon for ivaretakelse av liv og helse. Dette gjør spesialisthelsetjenesten trusselutsatt på lik linje med andre deler av totalforsvaret og kritisk infrastruktur. Forskningsdata, informasjon om beredskap, og sensitiv informasjon som helse- og personopplysninger er noen av verdiene som statlige aktører ønsker tilgang til [36] [24] [14] [1] [22]. Spesialisthelsetjenesten har tette forbindelser med ulike forskningsinstitusjoner, og forskning er en viktig og integrert del av helsesektoren. Globalt er det rapportert om interesse for medisinsk forskning fra statlige trusselsaktører [11] [4] [29] [30].

Foto: Christopher Lindseth Moen, Sykehuspartner HF.

Russland

Norges medlemskap i NATO, strategiske plassering og grense til Russland påvirker den vedvarende høye etterretningstrusselen fra Russland. Russiske EOS-tjenester har behov for informasjon som styrker egen situasjonsforståelse i dagens sikkerhetspolitiske situasjon, og Norges evne til å håndtere kriser spesielt hvor russiske interesser er involvert [1]. Russlands avhengighet til Kina blir stadig større som en konsekvens av de vestlige sanksjonene i forbindelse med krigen i Ukraina. Landene samarbeider kommersielt og innen forskning i Arktis [2] [17].

Vilje

Russland har høy vilje til å gjennomføre cyberspionasje mot norske mål. Både sivile og militære EOS-tjenester i Russland har informasjonsbehov knyttet til Norge. Dette inkluderer et varig behov for informasjon om totalforsvaret og beredskapsapparatet, som spesialisthelsetjenesten er en del av. Kritisk infrastruktur er et mål for russisk etterretning fordi tilgangen kan benyttes til spionasjeformål, eller til forberedelse av destruktive angrep som kan utnyttes i en tilspisset situasjon [22]. Spesialisthelsetjenesten har store mengder med helse- og personopplysninger som kan brukes som et virkemiddel innenfor spionasje og kan ha høy verdi for utenlandsk etterretning. Helseopplysninger kan brukes til å presse eller utnytte myndighetspersoner eller personer med høyt rettighets-nivå i IKT-systemer
[1] [3] [28] [30] [21].

Evne

Russiske cyberaktører bruker hele spekteret av tilgjengelige kapasiteter i gjennomføringen av cyberspionasje. Russiske cyberaktører har kapasitet til å infiltrere nettverk, infrastruktur, skytjenester og kan etablere full og vedvarende tilgang til ønsket infrastruktur. Russiske etterretningstjenester er kjent for å benytte ulike former for samarbeid mellom hacktivister og organiserte kriminelle miljøer, hensikten er å skjule hvem som står bak angrepet [4] [5] [6] [7] [31] [27] [22].

Kina

Kinesiske etterretningstjenester utnytter hele spekteret av cyberdomenet i sine cyberoperasjoner og bruker alle tilgjengelige verktøy og digital infrastruktur for å skjule sin egen aktivitet. Kinesiske myndigheter gjennomfører cyberspionasje i utstrakt grad mot blant annet myndigheter, forsvar og helse. Kina fortsetter å utfordre det vestlige fellesskapet på flere måter, der de søker å kontrollere strategisk infrastruktur, ressurser og verdikjeder. Kina jobber aktivt mot nordområdene, for å sikre fremtidig ressursutvinning og strategisk posisjonering [17] [2] [27] [22] [11] [32] [22].

Vilje

Kina har rettet en betydelig andel av sine cyberoperasjoner mot Vesten, og samtlige av Norges EOS-tjenestene forventer en økning av aktiviteten i Norge årene som kommer [33] [21]. Flere kinesiske trusselaktører har gjennomført globale cyberspionasjeaksjoner i 2023 [22] [27] [30]. Den amerikanske cybersikkerhetstjenesten (HC3) bekrefter at flere kinesiske trusselaktører har gjennom årene gjennomført cyberspionasje mot helsesektoren i USA og Sør-Europa, der angrepene har vært rettet mot blant annet medisinsk teknisk utstyr og medisinsk forskingsdata [29] [1] [2].

Evne

Kinesiske etterretningsorganisasjoner har evne til å gjennomføre avanserte cyberspionasjeoperasjoner. De har kapasitet til å infiltrere nettverk, infrastruktur, skytjenester og etablere full og vedvarende tilgang til informasjon og styringssystem. Kina vil utgjøre en betydelig etterretningstrussel mot norske virksomheter i tiden fremover [4] [19] [22] [33] [32] [34] [43].

Kinas kontraetterretningslov gir en svært bred forståelse av «etterretningsaktivitet», og omfatter innhenting av informasjon av betydning for investeringer og produksjon i Kina. Enhver kinesisk borger, virksomhet og organisasjon plikter ifølge loven til å bistå Kinas etterretningstjeneste ved behov. For kinesiske kommersielle teknologiselskaper betyr dette i praksis at all teknologi og kunnskap fra kinesiske selskaper kan bli tilgjengeliggjort for kinesiske myndigheter [2] [1].

Kina søker å utnytte sårbarheter i internetteksponerte tjenester for å etablere fotfeste i informasjonssystemer. I 2023 har det videre blitt observert en økning av mer sofistikerte målrettede phishing-kampanjer fra kinesiske trussel aktører. I løpet av 2023 er det observert at kinesiske aktører i større grad har benyttet seg av sosiale medier for sosial manipulering og rekruttering av innsidere [22] [27] [32].

Iran

Iran fokuserer i hovedsak sine cyberspionasjeoperasjoner mot sine regionale naboer, men har også angrepet europeiske land og USA. Iranske statlige aktører bruker stadig mer sofistikerte metoder og utnytter teknologi som er lett tilgjengelig. Dette inkluderer blant annet å skjule infrastruktur for kommando og kontroll (C2) av skadevare i offentlige skymiljøer, og de utnytter nulldagssårbarheter raskere [22] [4] [27] [9] [35] [36].

Vilje

Iran har gjennomført cyberspionasje mot forsknings- og utdannings-sektoren i Norge. Politiets sikkerhetstjeneste (PST) forventer at iranske aktører vil ramme norske virksomheter i 2024. Iranske aktører vil i året som kommer drive cyberspionasje som del av sin etterretningsaktivitet mot Norge. Norske virksomheter, inkludert spesialisthelsetjenesten, kan være mål for cyberspionasje fra iranske aktører [22] [1] [2].

Evne

Iran har betydelige evner til å gjennomføre cyberspionasje. I 2023 har Iran styrket sine kapabiliteter, og utnytter nulldagssårbarheter raskere. De har også gjennomført operasjoner i skymiljøer, hvor formålet er tilgang til informasjon eller bruke skymiljøet som verktøy for å etablere fotfeste [22] [36] [4] [35].

Iranske statlige aktører bruker regelmessig tilpassede verktøy i sine operasjoner. Verktøyene gir aktøren evnen til å etablere tilstedeværelse og unngå oppdagelse. Utnyttelse av nulldagssårbarheter i programvare hjelper trusselaktører å holde seg et skritt foran den som er angrepet. Iranske statlige aktører bruker tilpassede verktøy som gjør det mulig å etablere tilstedeværelse og unngå oppdagelse [22] [27].

Nord-Korea

Nordkoreanske cyberoperasjoner har blitt mer sofistikerte enn tidligere år, og begynner å nærme seg nivået til aktører fra Russland og Kina [22] [36].

Vilje

Nord-Korea trekkes fremdeles frem som en aktør som vil utføre cyberspionasje mot norske mål i 2024. Nord-Korea bruker i utgangspunktet cyberoperasjoner for å gjennomføre industrispionasje for å styrke landets forsvarsevne og øke Nord-Koreas svake økonomi. Nordkoreanske cyberaktører har stjålet informasjon fra norske virksomheter som kan skade norske sikkerhetsinteresser [1] [37] [22] [2] [38].

Evne

Nord-Korea har kapasitet til å gjennomføre cyberspionasje og har gjennomført flere vellykkede angrep mot finansinstitusjoner, militære og politiske organer i Vesten. Nord-Korea benytter offentlig kjent og egenutviklede skadevarer i cyberangrep. De utnytter sårbarheter blant annet i internetteksponerte tjenester, skytjenester og det har blitt observert kampanjer hvor målet er å få tilgang til påloggings-informasjon [22] [36].

Vurdering:

Cyberspionasje

Overordnet vurdering av trusselen fra cyberspionasje mot spesialisthelsetjenesten			
Land	**Vilje**	**Evne**	**Skadepotensiale**
Russland	Høy	Meget høy	Høyt
Kina	Høy	Meget høy	Høyt
Iran	Medium	Høy	Høyt
Nord-Korea	Meget lav	Høy	Høyt

Det vurderes som **sannsynlig** at statlige aktører har evne og vilje til å gjennomføre cyberspionasje mot spesialisthelsetjenesten i 2024. Det vurderes som **meget sannsynlig** at Russland og Kina har **høy** vilje til å gjennomføre cyberspionasje mot spesialisthelsetjenestens verdier, men de har ulike målsetninger med angrepene. Russlands fokus vil dreie seg om tilgang til informasjon som styrker deres generelle situasjonsforståelse, men også forhold til NATO-landene.

Det vurderes som **meget sannsynlig** at Russland har **høy** vilje til å utøve spionasje mot spesialisthelsetjenestens verdier som omfatter beredskap og krisehåndteringsevne.

Kinas fokus er rettet mot spionasje for å styrke egen økonomi og posisjon i verdensbildet. Det vurderes derfor som **sannsynlig** at Kina har vilje til å gjennomføre spionasje mot forskningsmiljøer, også innen spesialisthelsetjenesten.

Cyberspionasje mot spesialisthelsetjenesten er skadepotensiale vurdert til **høyt**, det å bli utsatt for cyberspionasje vil nødvendigvis ikke påvirke vår evne til å levere helsetjenester i regionene. Imidlertid kan det true konfidensialiteten og i verstefall tilgjengeligheten til informasjonen spesialisthelsetjenesten forvalter, og derfor også sikkerheten. Cyberspionasje fra russiske aktører vil utgjøre den største trusselen fra statlige aktører mot spesialisthelsetjenesten.

Det vurderes som **meget sannsynlig** at statlige aktørers EOS-tjenester innehar kapabiliteter gode nok til å omgå et godt grunnleggende sikkerhetsnivå.

Det vurderes som **meget sannsynlig** at statlige aktører har evne til å omgå sikkerhetsmekanismer ved å utnytte ikke allment kjente sårbarheter, såkalte nulldagssårbarheter.

3.2 Destruktive cyberangrep

Destruktive cyberangrep er i denne vurderingen definert som digitale angrep med hensikt å ødelegge eller forandre informasjon, data eller programvare slik at de ikke kan benyttes uten vesentlig gjenoppretting [12] [21].

En rekke stater har evne til å gjennomføre destruktive cyberangrep mot kritisk infrastruktur, som spesialisthelsetjenesten er en del av. Samtidig er det globalt observert nedgang i destruktive cyberangrep fra statlige aktører [22] [2] [27]. Gjennom verdikjedeangrep vil spesialisthelsetjenesten kunne bli påvirket av destruktive cyberangrep ved at underleverandør blir angrepet. Det har blitt registrert målrettede angrep mot underleverandører som har forbindelse til konfliktområder som krigen i Ukraina og nå i senere tid i Midtøsten [1] [12].

Hvis fremmede staters vilje til å bruke destruktive cyberangrep mot kritisk infrastruktur i Norge endrer seg, kan destruktive cyberangrep ramme spesialisthelsetjenesten med alvorlige konsekvenser. Spesialisthelsetjenesten kan også påvirkes av destruktive cyberangrep mot andre deler av kritisk infrastruktur eller underleverandører, som kraftsektoren eller vannforsyning [22] [34]. Statlige trusselaktørers vilje og evner varierer, de bruker ofte lignende eller samme metoder når de distribuerer cyberangrep.

I utgangspunktet har helse et vern mot angrep gjennom Genèvekonvensjonene. Imidlertid har det blitt bekreftet i at russiske styrker har angrepet feltsykehus og ambulanser i Ukraina. I tillegg er det bekreftet av FN at Israel har angrepet på helseinstitusjoner i Gaza [39] [31]. Risikoen er at slike angrep kan skape en presedens som i større grad enn før legitimerer helse som mål i konflikter og krig. Denne utviklingen kan føre til at terskelen for å gjennomføre destruktive cyberangrep mot helse reduseres.

Russland

Vilje

Russiske statlige aktørers vilje til å gjennomføre destruktive angrep er i hovedsak for å støtte andre typer maktmidler. Viljen til å gjennomføre destruktive angrep mot norske mål er lav, og det observeres en generell nedgang globalt. Dette har sammenheng med økningen som skjedde i forbindelse med angrepet på Ukraina. Trusselen kan øke igjen i en skjerpet sikkerhetspolitisk situasjon eller militær konflikt [1] [2] [3] [22].

Evne

Russland har meget høy evne til å gjennomføre destruktive cyberangrep og har over tid praktisert slike angrep. I Russlands hybride krigføring mot Ukraina har russiske aktører gjennomført en rekke destruktive cyberangrep mot kritisk infrastruktur i landet. Russland er kjent for å bruke stedfortredere, som cyberkriminelle eller hacktivist-grupper, for å gjennomføre ulike typer cyberangrep [4] [40] [19] [22] [3] [27].

Kina

Vilje

Kinas vilje til å gjennomføre destruktive cyberangrep mot spesialisthelsetjenesten er uendret fra fjoråret. Imidlertid kan endring i kinesiske interesser påvirke viljen til å gjennomføre destruktive cyberangrep. [22] [27] [32].

Evne

Kina har evne til å gjennomføre destruktive cyberangrep. I 2023 oppdaget sikkerhetsmyndigheter i USA at kinesiske aktører hadde vært inne i flere datasystemer tilknyttet kritisk infrastruktur [33]. Amerikanske EOS-tjenester vurderte med stor sikkerhet at aktøren forhåndsposisjonerte seg på IT-nettverk for å forstyrre funksjoner i fremtiden. Aktørens valg av mål og atferdsmønster var ikke i samsvar med tradisjonell cyberspionasje eller etterretningsinnsamlingsoperasjoner [8] [22]. En viktig del av Kinas militære cyberstrategi er å kunne gjennomføre destruktive cyberangrep for å binde en nasjons ressurser til en intern krise som vil skifte fokus fra en konflikt mot Kina [33] [22] [27] [32].

Iran

Vilje

Iran fokuserer i hovedsak sine destruktive cyberangrep mot egen region, men har gjennomført angrep mot USA og land i Europa [35]. Iranske aktører har aktivt gjennomført slike angrep i mange år, blant annet mot Saudi Arabia og Israel [4]. Med angrepene mot mål i USA og Albania kan man se økt vilje til å gjennomføre slike angrep mot land som Iran oppfatter at jobber mot iranske interesser. Det er observert et skifte fra destruktive operasjoner til cyberspionasje fra Iran [22].

Evne

Iranske aktører har demonstrert betydelig evne i gjennomføring av destruktive cyberangrep, blant annet mot Saudi Arabia og Israel. Iran bruker også cyberdomenet aktivt mot stater som rammer eller jobber mot Iranske interesser. Iran har historisk fokusert sine operasjoner mot myndigheter, industri, infrastruktur og helse. Det siste året har Iran styrket sine kapabiliteter og har i større grad gjennomført operasjoner i skymiljøer i tillegg til å unytte nulldagssårbarheter raskere [27] [22] [35].

Nord-Korea

Vilje

Nord-Korea har i utgangspunktet økonomiske motiver i sine operasjoner, og dette har ikke endret seg. Nordkoreanske aktører har gjennomført målrettet angrep mot selskaper innenfor kryptovaluta, men benytter også utpressingsverktøy [22] [38].

Evne

Nord-Koreas fokus på økonomisk vinning har landet opparbeidet seg en betydelig kapasitet som kan benyttes til å gjennomføre destruktive cyberangrep. De benytter offentlig tilgjengelige, samt egenutviklede verktøy og skadevare. Nordkoreanske aktører utnytter sårbarheter i internetteksponerte tjenester, og det har blitt observert kampanjer der målsetningen er å få tilgang til påloggingsinformasjon for å benytte disse i senere destruktive cyberangrep [22] [36].

Vurdering:

Destruktive cyberangrep

Overordnet vurdering av trusselen fra destruktive cyberangrep i spesialisthelsetjenesten

Land	Vilje	Evne	Skadepotensiale
Russland	Lav	Meget høy	Meget høyt
Kina	Meget lav	Meget høy	Meget høyt
Iran	Meget lav	Høy	Meget høyt
Nord-Korea	Meget lav	Høy	Meget høyt

Destruktive cyberangrep har **meget høyt** skadepotensiale for spesialisthelsetjenesten, fordi systemer blir utilgjengelige, eller at sensitiv informasjon blir kompromittert. Trusselaktørene har **høy** til **meget høy** evne til å gjennomføre denne typen angrep.
På bakgrunn av EOS-tjenestene sine nasjonale vurderinger kan det ikke utelukkes forsøk på å etablere tilstedeværelse i vår kritiske infrastruktur for fremtidige destruktive cyberangrep. Det vurderes som **mulig** med **lav konfidens** at spesialisthelsetjenesten kan være utsatt for forsøk fra aktører som ønsker å posisjonere seg i operasjonell teknologi (OT) for senere å gjennomføre destruktive cyberangrep eller digital sabotasje.

Russland har **meget høy** evne til å gjennomføre destruktive cyberangrep, men viljen vurderes som **lav**, imidlertid kan trusselen stige i forbindelse med en skjerpet politisk eller militær konflikt. Viljen til å gjennomføre destruktive cyberangrep mot spesialisthelsetjenesten fra Kina, Iran og Nord-Korea, vurderes til **meget lav** og det er **meget lite sannsynlig** at aktørene gjennomfører angrep slik situasjonen er i dag.

Foto: Shutterstock

3.3 Påvirkningsoperasjoner

En påvirkningsoperasjon er en samordnet innsats for å påvirke en meningsdannelse hos enkeltpersoner eller grupper gjennom tilgjengelige verktøy, som sosiale medier, falske nyheter eller påvirkning av tjenester [41] [26]. Statlige aktører har i større grad brukt cyberdomenet til å spre sine narrative og fronte sine verdier til et større publikum. Det er rapportert mange eksempler på dette i den pågående krigen i Ukraina, hvor russiske aktører bruker sosiale medier for å spre sin versjon av krigen. Rapporter indikerer en lignende trend i kinesiske kampanjer, hvor de har tatt i bruk nye språk og sprer seg veldig raskt på sosiale medier.

Påvirkningsoperasjoner kan rettes mot hele samfunnet og fordi påvirkningsoperasjoner er fordekte, kan aktørene utnytte de fleste digitale plattformer og sosiale medier [2] [1] [42] [22]. Russland har demonstrert betydelige evner til å gjennomføre påvirkningsoperasjoner gjennom statlige ressurser, men de benytter ofte hacktivister og kontrollerte medier for å spre desinformasjon [3] [9] [27].

Kina anser påvirkningsoperasjoner som viktig del av sin propagandavirksomhet og gjennomføres ofte av private eller kinesiske mediefirmaer. Dette gjelder fra overvåkning internt i Kina, til regionale eller internasjonale kampanjer [22] [27] [30].

Vurdering:
Påvirkningsoperasjoner

Det vurderes som **lite sannsynlig** at spesialisthelsetjenesten vil bli utsatt for målrettede påvirkningsoperasjoner fra Russland og Kina. Aktørene har **meget høy** evne til å gjennomføre denne typen operasjoner. Viljen til å gjennomføre påvirkningsoperasjoner mot spesialisthelsetjenesten er **lav** med lav konfidens.

Dersom det er fordelaktig for russiske interesser å undergrave norsk helsevesen, kan dette også ramme spesialisthelsetjenesten. Videre kan Russland anse det fordelaktig å svekke tilliten til norske myndigheter, dersom den sikkerhetspolitiske situasjonen forverrer seg.
I en slik situasjon vurderes det som mulig at spesialisthelsetjenesten trekkes inn i en påvirkningsoperasjon.

Foto: Max Bender, Unsplash

Kapittel 4

Hacktivister

Hacktivister, eller cyber-aktivister, kan være enkeltindivider eller grupperinger hvis motivasjon er å formidle et holdningsmessig eller politisk budskap gjennom et digitalt angrep. Den typiske hacktivist-operasjonen benytter tjenestenektangrep (DDoS) eller kompromittering av en hjemmeside for å vise sin støtte til en sak. Eksempler på dette kan være motstand mot politisk betente emner eller pågående geopolitiske konflikter. Hovedmomenter i hacktivismeaktivitet det siste året har vært krigen mellom Ukraina og Russland og krigen i Gaza.

Etter en stabilisering i det pro-russiske hacktivistlandskapet det siste året, kom pro-palestinske hacktivistgrupper frem i lyset etter eskaleringen i konflikten på Vestbredden oktober 2023. Sammen med idealistiske hacktivistgrupper dukket det samtidig opp flere "*faketivister*" - statlige grupperinger som gjemmer seg bak hacktivist-merkelappen, som etterligner retorikken og mediebruken til eksisterende grupper for å passe inn i hacktivistlandskapet [4]. Det er gode indikasjoner på at både Russland og Iran, enten direkte eller indirekte, står bak flere "*faketivist*"-grupper [1].

Vilje
Hacktivister har utvist en lavere vilje til å angripe helsesektor det siste året. Norsk helsesektor har heller ikke nå vært et prioritert mål, og vi kan ikke se at helsesektor internasjonalt har vært spesielt prioritert over andre sektorer, der finans og transport har blitt rammet hardest.

Som året før, ser vi at flere grupper er mer opptatt av å bygge opp et varemerke og skape inntrykk av å ha en effekt, enn å ha en reell virkning [43]. Vi observerer at enkelte pro-russiske grupper har beveget seg bort fra å gjennomføre angrep, og hovedsakelig formidler propaganda fra det russiske statsapparatet. Dette kommer gjerne etter en endring i ledelsen i gruppen, og frafall av sentrale ressurser som hadde kompetansen til å gjennomføre angrepene [43]. De norske EOS-tjenestene forventer at hacktivister vil angripe Norge også det kommende året, dette har sammenheng Norges støtte til Ukraina og medlemskap i NATO [1] [2].

Evne
Hacktivisters evne til å utgjøre en trussel varierer kraftig. Enkelte grupper er ikke i stand til å utføre mer enn forstyrrende DDoS-angrep, mens andre har kapasiteten til å gjennomføre større koordinerte operasjoner og kompromittere utvalgte mål. Et eksempel på et slikt angrep er da den pro-palestinske gruppen AnonGhost kompromitterte en Israelsk app for varsling av angrep, og sendte ut falskt varsel om angrep med atomvåpen [44].

Under DDoS-angrep mot norske organisasjoner vil mange mål innføre geoblokkering eller vask av trafikken. Dette kan gjøre at trusselaktøren får inntrykk av å ha tatt ned målet, selv om det i realiteten er tilgjengelig for vanlige besøkende som opplever kun mindre forstyrrelser.

Få grupper har vist en evne til å ta ned større tjenester og nettsider, og de med kapabiliteten vet å utnytte den økonomisk. Flere grupper har begynt å tilby tjenestene sine til høystbydende og dermed gått bort fra den politiske overbevisningen gruppen ble grunnlagt på. Der gruppene liker å skryte av å ha tatt ned et mål, ser vi også at det gjennomføres et stort antall angrep der målet er tilstrekkelig beskyttet og opplever ingen nedetid [43].

Disse angrepene annonseres ikke av gruppene, noe som gir gruppens følgere et skjevt bilde av gruppens aktiviteter. At feilslåtte angrep ikke annonseres gjør det vanskeligere å vurdere gruppenes reelle evne til å gjennomføre angrep, da vi mangler det totale bildet.

Man har likevel det siste året sett en økning i evne hos enkelte grupperinger, der flere store vellykkede angrep har blitt gjennomført. Store organisasjoner må ofte godta trafikk fra hele verden og kan ikke beskytte seg med enkle midler, som geoblokkering. Med stor og langvarig nedetid og forstyrrelser i tjenester hos Microsoft og nedetid på nettsidene og mobil-appen til SAS, ser vi at noen kategorier av tjenester er sårbare for enkle virkemidler som utnyttes til det fulle av de mer kompetente hacktivistene [7].

Vurdering:
Hacktivister

Overordnet vurdering mot spesialisthelsetjenesten: **Hacktivister**			
	Vilje	**Evne**	**Skadepotensiale**
Hacktivister	Medium	Lav	Lavt

Hacktivisters vilje til å forsøke å ramme spesialisthelsetjenesten vurderes til **medium.** Det er viktig å være bevisst på at viljen til hacktivistgrupper kan endre seg raskt med bakgrunn i skiftende geopolitisk situasjonsbilde, betente mediesaker eller andre saker som kan fange hacktivisters oppmerksomhet. Vi ser en klar sammenheng mellom mediesaker og hvordan det fremprovoserer prioriterte mål. Felles for disse er at jo mer oppmerksomhet sakene får i internasjonale og russiske medier, desto mer sannsynlig er det at hacktivister bruker sakene som et påskudd for å gjennomføre angrep.

Vi vurderer det som **meget sannsynlig** at skadepotensialet av et tjenestenektangrep fra hacktivister vil være **lavt** og kortvarig. Det vurderes som **meget lite sannsynlig** at disse angrepene vil få konsekvenser for pasientbehandling.

Evnen til hacktivister er vurdert til å være **lav**, sammenlignet med andre trusselaktører omtalt i denne rapporten. Vi vurderer det som **sannsynlig** at enkelte hacktivistgrupper vil utvikle seg til å inneha en større organisatorisk kompetanse, og dermed øke evnen til å koordinere og gjennomføre større angrep.

Foto: Shutterstock

Kapittel 5

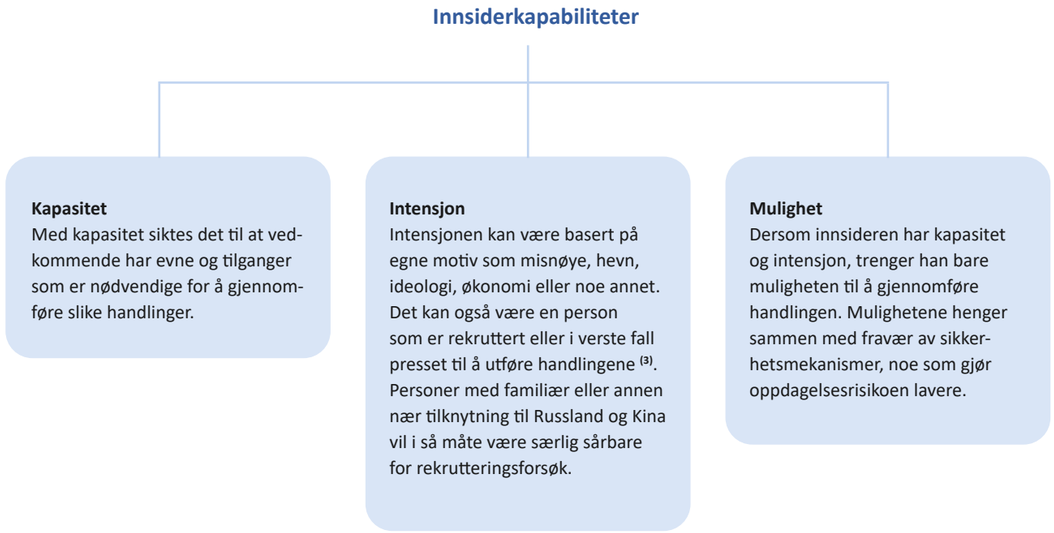
Innsidere

Denne aktørgruppen skiller seg ut fra de andre trusselaktørene som er vurdert i denne rapporten i den forstand at de har legitim tilgang til vår infrastruktur. Temaet er viktig å vite noe om for alle sektorer. Dette inkluderer også spesialisthelsetjenesten, som alene består av ca. 137 000 årsverk. Dette kapittelet skal derfor gi økt innsikt om temaet.

Samtlige av EOS-tjenestene melder om at det er forventet økt etterretningsaktivitet som følge av den nåværende sikkerhetspolitiske situasjonen. Russland vil utgjøre den største etterretningstrusselen i Norge, men også Kina vil utgjøre en betydelig og økende trussel. Cyberoperasjoner og rekruttering av innsidere vil være blant de mest sentrale metodene for statlige aktører i 2024, og det forventes at Russland og Kina vil være spesielt aktive i sine forsøk på å rekruttere kilder og innsidere [1] [2] [3].

En trend som fremheves er at bruk av innsidere vil få økt verdi mot virksomheter som har god digital sikkerhet. En trusselaktør som aksepterer økt risiko, har mer å vinne og mindre å tape på å utnytte menneskelige sårbarheter for å få tilgang til sensitiv informasjon. En trusselaktør vil sannsynlig velge minste motstands vei mot målet, og heller betale en ansatt for informasjon, enn å bruke avanserte verktøy for å bryte seg inn [40] [3] [45].

Det er et for lavt kunnskapsnivå i virksomheter om hva en innsider er, hvordan de opererer, samt trusselbildet rundt innsidevirksomhet. Dette gjør at oppdagelsesrisikoen er lavere, blant annet fordi det uten slik kunnskap vil bli vanskelig å gjennomføre tilstrekkelige sikkerhetstiltak [46].



Kapasitet, intensjon og mulighet
En innsider i denne rapporten er som ordet tilsier en person "på innsiden" av virksomheten, og som bruker sine legitime tilganger til å skade virksomheten eller for egen vinning. En innsider har i utgangspunktet kapasitet, intensjon og mulighet til å utføre uønskede handlinger mot virksomheten.

For eksempel kan en leder, forvalter eller annen person med utvidede tilganger enklere kunne hente ut sensitiv informasjon uten å vekke mistanke. Mulighetsrommet for en innsider vil også være større i systemer uten logging eller der det mangler tilgangsstyring.

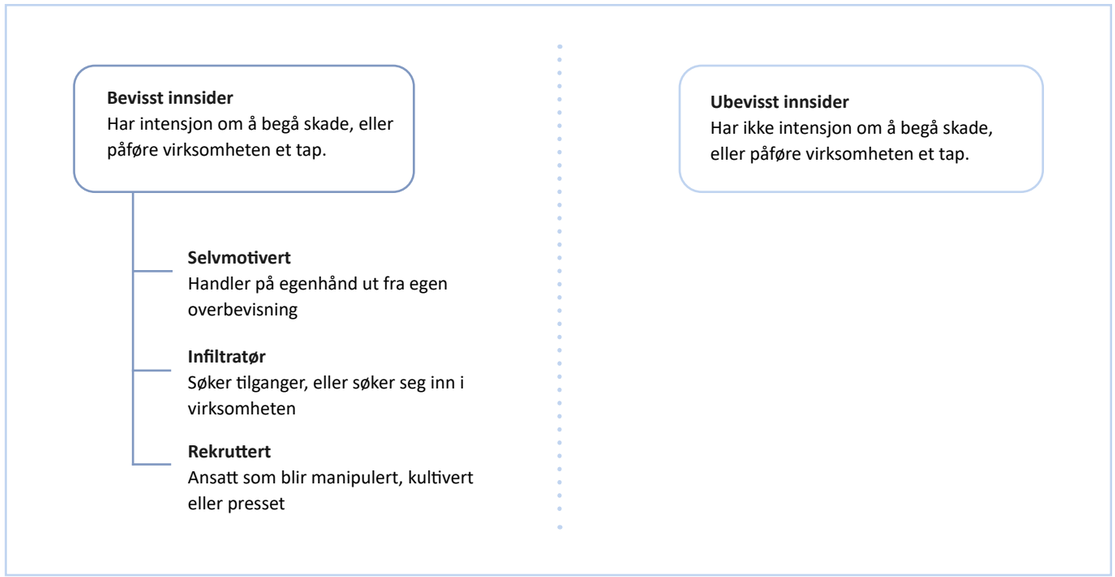
Kategorier av innsidere
Det kan med andre ord variere hva en innsider er, og det kan derfor være nyttig å kategorisere disse for å gjøre trusselen håndterbar.

Innsidere i en organisasjon kan variere fra de som ubevisst kan forårsake skade, til de som aktivt søker å skade virksomheten de jobber for. En ubevisst innsider mangler intensjonen om å skade, men kan blir brukt uten at vedkommende vet det selv. Muligheten til å gjøre skade henger da sammen med hvor bevist forhold innsideren har til informasjonssikkerhet, og sikkerhetskulturen i organisasjonen. En bevisst innsider er en person som har til hensikt å begå skadelige handlinger. Blant bevisste innsidere finner vi selvmotiverte innsidere, infiltratører og rekrutterte innsidere.

Selvmotivert innsider
En selvmotivert innsider har, som ordet antyder, motivert seg selv til å bli en innsider. Motivasjonen kan drives av personlige grunner, som for eksempel økonomisk gevinst eller ideologiske overbevisninger. Disse innsiderne kan også bli påvirket av desinformasjon som sprer seg i samfunnet, noe som kan endre deres oppfatninger og holdninger, og gjøre dem mer mottakelige for rekruttering.

Den generelle spredningen av desinformasjon i samfunnet kan endre enkeltpersoners oppfatninger, holdninger og handlinger gjennom feilaktig eller villedende informasjon (27) (1). Slik påvirkning kan også foregå på virksomhetsnivå, og ikke nødvendigvis direkte mot enkeltpersoner. Man kan forsøke å redusere lojaliteten til virksomheten gjennom tema som opptar enkelte grupper i virksomheten. For eksempel var det under massevaksineringen mot korona flere grupper som sto frem som mistroiske mot det offentlige helsevesenet (49).

Infiltratør
Infiltratører er en annen gruppe som i utgangspunktet ikke har kapasitet idet vedkommende blir rekruttert, men må posisjonere seg for å få dette. Dette kan for eksempel være en person som søker på en utlyst stilling, eller en ansatt som søker en annen stilling internt i virksomheten. Det kan også være en ansatt som søker utvidede tilganger slik at vedkommende kan få tilgang til informasjon, og derved nødvendig kapasitet.



Rekruttert innsider
Rekrutterte innsidere kan ha blitt manipulert, påvirket eller presset til å utføre innsidehandlinger av en ekstern aktør. Rekrutteringsprosessen foregår gjerne i fire faser: Kontaktetablering, vurdering av egnethet, kultivering/press og rekruttering. Tidligere foregikk slike rekrutteringsprosesser primært gjennom fysiske møter. Konferanser er fremdeles populære arenaer for kontaktetablering av mulige kilder. I dag bruker trusselaktører i økende grad sosiale medier og chatteapplikasjoner til rekruttering av kilder. I tillegg kan sosiale medier være en kilde til informasjon som kan brukes mot vedkommende (1) (22).

Dersom personen vurderes som egnet til å fungere som en innsider, er neste fase å kultivere et forhold til vedkommende. De kan tilby gaver eller andre fordeler, eller utøve press basert på informasjon eller svakheter de har oppdaget om personen. Til slutt kommer selve rekrutteringen, der vedkommende enten frivillig eller under tvang aksepterer å fungere som en innsider i virksomheten.

Vurdering:
Innsidere

EOS-tjenestene vurderer at rekruttering av innsidere spesielt fra Kina og Russland vil utgjøre en høy trussel for norske virksomheter. I tillegg er virksomheter innenfor helsesektoren definert som ett av hovedmålene til statlige trusselaktører. Vi ser også en trend der bruk av innsidere har økt verdi mot virksomheter som har god digital sikkerhet.

Vi vurderer derfor at sannsynligheten for at spesialisthelsetjenesten vil oppleve uønsket hendelse som følge av innsider er **meget sannsynlig**. Skadepotensialet til en innsider vil variere basert på evne og mulighet. Dette kommer an på blant annet rettighetsnivå til systemer, teknisk kunnskap og myndighet. Skadepotensialet vil derfor kunne variere fra **meget lavt** til **meget høyt**.

Foto: Shutterstock

Kapittel 6

Cybersikkerhetsutfordringer

Samfunnet blir stadig mer datadrevet, og med dette følger også nye sårbarheter. Informasjons- og kommunikasjonsteknologi har en viktig funksjon for å oppnå verdiskaping og beskytte verdiene mot sikkerhetstruende hendelser, som cyberoperasjoner. Derfor er tillitt til IKT-systemene avgjørende, og motstandsdyktighet mot digitale angrep vesentlig for spesialisthelsetjenesten. Truslene utvikler seg like raskt som gevinstene med teknologien vi benytter. Et mulighetsrom for spesialisthelsetjenesten vil også kunne gi et mulighetsrom for en trusselaktør.

I dagens trusselbilde handler derfor responsen mot trusler om prioritering og organisasjonens innsats. Dette innebærer at man må prioritere kjente og skadelige trusler samtidig som man må forberede seg på ukjente trusler.

Skytjenester
Bruk av skytjenester øker i omfang, noe som øker kompleksiteten og angrepsflaten. Skytjenester er gjerne tett integrert med interne IKT-systemer, der en slik hybrid tilnærming kan skape utilsiktet ekstern eksponering av interne tjenester. Samtidig gir skytjenester store muligheter for realisering av gevinster fra teknologiutvikling og digitalisering, samt at det kan bidra til bedre sikkerhet.

Bruk av skytjenester vil med andre ord kunne gi virksomheter større mulighetsrom og sikkerhetsmessige fordeler, men kan også føre til en sentralisering av verdier, og dermed bli et mer ettertraktet mål blant trusselaktører som er drevet av profitt og statlige aktører [8]. Virksomheter bør videre ha en bevist tilnærming til avhengigheter som skapes til leverandører og bygge kompetanse for å hente ut nødvendige sikkerhets-messige gevinster på kort og lang sikt.

Kunstig intelligens (KI)
Kunstig intelligens er systemer som utfører handlinger, fysisk eller digitalt, basert på tolkning og behandling av strukturerte eller ustrukturerte data for å oppnå et spesifikt mål [50]. Virksomheter må ta i bruk kunstig intelligens på en trygg og ansvarlig måte, noe en trusselaktør ikke er bundet av. Dette skaper ujevne odds mellom oss og trusselaktørene, ved at de kan ta i bruk teknologien raskere.

Bruk av KI har potensiale til å transformere næring og samfunn, men er også sårbare for angrep og utnyttelse. En KI-modell kan produsere feil resultater basert på inngangsverdier, eller repetere biaser i datasett KI modellen har blitt trent på.

Utfordringene med KI for spesialisthelsetjenesten er flere, og tross at teknologien er forsket på lenge, er teknologien fortsatt umoden og man har lite erfaring med den over tid. En utfordring er at man ikke vet hvordan en KI-modell skal «glemme» eller avlæres.

KI vil øke våre evner til å oppdage trusler innen cyberdomenet vil det også i stor grad øke evnene til trusselaktørene til å gjennomføre cyberangrep uoppdaget. Ved bruk av KI kan trusselaktører automatisere deler av eller hele angrepsprosessen, rekognosering, målretting og utnyttelse. KI-styrte angrep kan tilpasse seg miljøet i målet som gjør dem vanskeligere å oppdage og motvirke [52] [51].

Trusselaktører fortsetter å utnytte bruk av KI til å utvikle sine metoder og verktøy, og vi ser allerede eksempler på bruk av KI i direktørbedrageri. Gjennom 2023 ser vi også at kunstig intelligens for alvor kom inn i det offentlige ordskiftet. Dette viser at kunstig intelligens kan understøtte flere kriminalitetsområder. Når cyberkriminelle tar i bruk nye verktøy kan andre raskt følge etter, noe som øker cyberkriminelle sine kapabiliteter hurtig [8]. Samtidig som kapabilitetene til de cyberkriminelle øker, vil KI også kunne bidra i eksponering av virksomheters svakheter for disse aktørene. Gjennom KI-støttet rekognosering og målretting vil en trusselaktør avdekke grunnleggende sikkerhetssvakheter hos et mål raskere.

En av konsekvensene av dette er at store datasett med sensitiv og verdifull informasjon vil sannsynlig bli mer ettertraktede mål for trusselaktører [25]. Datasett kan brukes til maskinlæring for å trekke ut sammenhenger som ellers er vanskelig tilgjengelig for ufaglærte. Slike databaser kan være offentlige helseregistre, folkeregistre eller registre over kritisk infrastruktur.

Løsninger basert på KI er på vei inn i pasientbehandlingen, men det fordrer en trygg og god ibruktagelse som ivaretar personvern og informasjonssikkerhet. Ettersom tilliten til KI vokser, vil avhengigheten til teknologien øke. Det er viktig å være bevisst på at bruk av kunstig intelligens kan endre arbeidsprosesser og behandlingsforløp.

Nulldagssårbarheter og raskere utnyttelse
Nulldagssårbarheter refererer til at det er en ukjent sårbarhet eller feil i programvare, som trusselaktørene gjerne oppdager før leverandøren [3]. Et sentralt utviklingstrekk innenfor cyberdomenet er utnyttelse av slike nulldagssårbarheter, og det er vanskelige å beskytte seg mot dette [8].

Nulldagssårbarheter er ofte krevende å avdekke, og det er gjerne kompetente trusselaktører som klarer å avdekke disse. Slike sårbarheter selges hovedsakelig kommersielt for store pengesummer. Nulldagssårbarheter vil sannsynligvis få økt verdi blant cyberkriminelle, og kunne øke skadepotensialet. Statlige aktører og organiserte kriminelle er kjent for å utnytte slike sårbarheter, og trenden med økende utnyttelse er forventet at fortsetter i tiden fremover [8, 14].

Sosial manipulering
Sosial manipulasjon er en tradisjonell måte å angripe virksomheter på, og teknologi er på mange måter en moderne måte utføre denne typen angrep gjennom. Likevel må det forventes at metodene vil fortsette å utvikle seg. Globalt ser man en begynnende trend der trusselaktører i større grad søker å bygge en form for tillitt hos sine mål først, før man forsøker å få vedkommende til å utføre en handling som muliggjør installering av skadevare. En informert, motivert og sikkerhetsbevisst ansatt vil fremdeles være et av de viktigste sikkerhetstiltakene mot fremtidens cybertrusler.

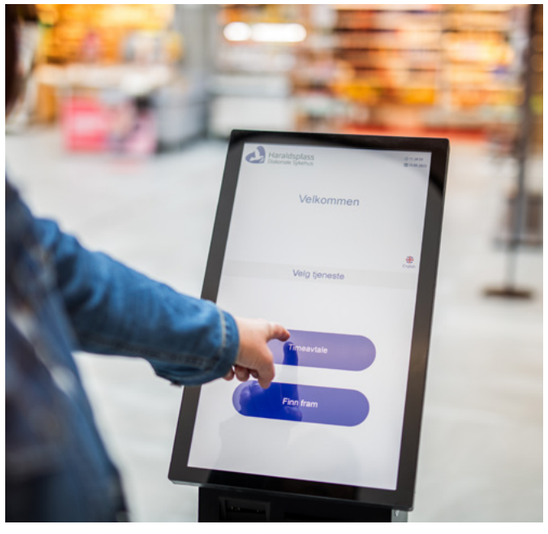


Foto: Ingvild Festervoll Melien / Helse Vest IKT

Referanseliste

1. **PST.** *Nasjonal trusselvurdering 2024.* Oslo : PST, 2024.

2. **Etterretningstjenesten.** *FOKUS 2024 Etterretningstjenestens vurdering av aktuelle sikkerhetsutfordringer.* Oslo : Etterrettningstjenesten, 2024.

3. **NSM.** *Risiko 2024 Nasjonal sikkerhet er et felles ansvar.* Oslo : NSM, 2024.

4. **Crowdstrike.** *Global Threat Report 2024.* s.l. : Crowdstrike, 2024.

5. **Recorded Future: Insikt Group.** *Dark Covenant 2.0: Cybercrime, the Russian State, and the War in Ukraine.* s.l. : Recorded Future, 2023. CTA-RU-2023-0131.

6. **Recorded Future.** *Dark Covenant: Connections Between the Russian State and Criminal Actors.* s.l. : Recorded Future, 2021. CTA-RU-2021-0909.

7. **Mandiant Advantage.** *License to KillNet: Hacktivists Expand Targeting Beyond Eastern Europe.* s.l. : Mandiant Advantage, 2022. 22-00020786V2.

8. **Kripos.** *Cyberkriminialitet 2024.* s.l. : Kripos, 2024.

9. **Center for Cybersikkerhed CFCS.** *Trusselsvurdering Cybertruslen mod Danmark 2023.* s.l. : CFCS, 2023.

10. **Flare.** Bleeping Computer. *The Initial Access Broker Economy: A Deep Dive into Dark Web Hacking Forums.* [Internett] 07 09 2023. [Sitert: 01 04 2024.] https://www.bleepingcomputer.com/news/security/the-initial-access-broker-economy-a-deep-dive-into-dark-web-hacking-forums/.

11. **Check Point.** *2024 Cyber Security Report.* s.l. : Check Point Research, 2024.

12. **Center for cybersikkerhed.** *Cybertruslen mod sundhedssektoren.* s.l. : Center for cybersikkerhed, 2023.

13. **Politiet.** *Politiets trusselvurdering 2023.* Oslo : POD, 2023.

14. **HelseCERT,** *Intern Kilde.*

15. **Nordic Financial CERT.** *Cyber Threat Landscape for the Nordic Financial Sector.* s.l. : Nordic Financial CERT, 2024.

16. **Politiet.** *Politiets trusselvurdering 2024.* Oslo : POD, 2024.

17. **Justis- og beredskapsdepartementet.** *NOU 2023: 17 Nå er det alvor — Rustet for en usikker fremtid.* Oslo : Regjeringen.no, 5. juni 2023.

18. **Crowdstrike.com.** *Cyber Big Game Hunting.* [Internett] 22 Februar 2024. [Sitert: 23 04 2024.] https://www.crowdstrike.com/cybersecurity-101/cyber-big-game-hunting/.

19. **Mandiant.** *M-TRENDS 2023 Mandiant Special Report.* s.l. : Manidant part of Google Cloud, 2023.

20. **CERT-EU.** *Threat Landscape Report 2023.* Brussel : EU, 2023.

21. **Spesialisthelsetjenesten.** *Trusselvurdering Det digitale trusselbildet mot spesialisthelsetjenesten.* s.l. : Sykehuspartner, 2023.

22. **Microsoft.** *Microsoft Digital Defense Report.* s.l. : Microsoft, 2023.

23. **Crowdstrike.** *2024 Global Threat Report.* s.l. : Crowdstrike, 2024.

24. **Den Norske Bank DNB.** *Finansiell trygghet i en usikker verden. Trusler og trender fra et DNB-Perspektiv 2024.* Oslo : DNB, 2024.

25. **European Union Agency for Cybersecurity.** *ENISA Threat Landscape 2022.* Brussel : EU, 2022.

26. **PST.** *Nasjonal trusselvurdering 2023.* Oslo : PST, 2023.

27. **Crowdstrike.** *2023 Global Threat Report.* s.l. : Crowdstrike, 2023.

28. **Mandiant Advantage.** *Country Snapshot: Norway (Q4 2023).* s.l. : Mandiant Advantage, 2024.

29. **Health Sector Cybersecurity Coordination Center.** HC3: Threat Profile August 16, 2023 TLP:CLEAR Report: 202308161700. s.l. : Health Sector Cybersecurity Coordination Center, 2023.

30. **Mandiant Advantage.** *Industry Snapshot: Healthcare (Q4 2023).* s.l. : Mandiant Advantage, 2024.

31. **Mandiant. Country Profile:** *Russia (2023).* s.l. : Mandiant Advantage, 2023.

32. **Mandiant. Country Profile:** *China (2023).* s.l. : Mandiant Advantage, 2023.

33. **CISA ASD NSA GCHQ CCCS ACSC.** *PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure.* s.l. : CISA, 2024.

34. **CISA FBI NSA GCSB CCCS ACSC ASG.** *People`s Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection.* s.l. : CISA, 2023.

35. **Mandiant Advantage.** *Country Snapshot: Iran (Q4 2023).* s.l. : Mandiant Advantage, 2023.

36. **Crowdstrike.** *2023 Cloud Risk Report.* s.l. : Crowdstrike, 2023.

37. **PST .** *"Indikatorer på ulovlige anskaffelser" (24. Aug. 2023) PST. <pst.no/alle-artikler/artikler/ulovlige-anskaffelser-og-indikatorer/>* . s.l. : PST, 2023.

38. **Mandiant Advantage.** *Country Snapshot: North Korea (Q4 2023).* s.l. : Mandiant Advantage, 2023.

39. **Marius Nyquist Pedersen, Tor Ole Vormdal, Marit Lind, Thor Engøy.** *FFI- Rapport Fremtidens sanitet effektiv ressurs i Forsvaret og totalforsvaret. Oslo : FFI, 2022.* 22/01114.

40. **NSM.** *NSM Nasjonalt digitalt risikobilde 2023.* s.l. : NSM, 2023.

41. **Bergh, Arild.** *Understanding Influence Operations in Social Media:. Journal of Information Warfare (2020)* 19.4: 110-131. 2020.

42. **FFI.** *Teknologiske og samfunnsmessige utviklingstrekk av betydning for nasjonale sikkerhetsinteresser i et 2030-perspektiv.* s.l. : FFI, 2023.

43. **HelseCERT.** *Intern kilde.*

44. **CyberMaterial.** *AnonGhost Hacks Red Alert App.* 2023.

45. **CISA Cybersecurity and Infrastructure Security Agency.** *Insider Threat Mitigation Guide.* s.l. : CISA, 2020.

46. **NSM.** *Temarapport Innsiderisiko.* Oslo : NSM, 2020.

47. **Mandiant Advantage.** *Country Snapshot: The Nordic Region Q4 2023.* s.l. : Mandiant Advantage, 2023.

48. **Palo Alto UNIT42.** *Incident Response Report 2024.*

49. **Politiet Kripos NC3.** *Temarapport: Generativ kunstig intelligens og cyberkriminalitet.* OSLO : Kripos, 2023.

50. **ØKOKRIM.** *okokrim.no. webområde for Økokrim.* [Internett] 3 4 2024. [Sitert: 3 April 2024.] https://www.okokrim.no/bedrageri.549300.no.html.

51. **National Cuber Security Centre & National Crime Agency.** *Ransomware, extortion and the cyber crime ecosystem: A white paper from the NCSC and the National Crime Agency (NCA).* s.l. : NCSC, 11 September 2023.

52. **Mandiant Advantage.** *Trust Me I`m a Professional: The Evolution and Commoditization of the Cyber Crime Ecosystem.* s.l. : Mandiant Advantage, 2021. 21-00012276.

53. **ESET Research.** *Threat Report.* s.l. : ESET, H2 2023.

54. **Check Point.** *Cyber Security Report.* s.l. : Check Point, 2023.

55. **ESET.** *Cybersecurity Trends 2023: Securing our hybrid lives.* s.l. : ESET, 2023.

56. **Mandiant Advantage.** *Industry Snapshot: Goverment (Q4 2023).* s.l. : Mandiant Advantage, 2023.

57. **Mandiant. Country Snapshot:** *China (Q4 2023).* s.l. : Mandiant Advantage, 2023. 24-10000016V1.

58. **Chainalysis.** *The 2023 Crypto Crime Report: Everything you need to know about cryptocurrency-based crime.* s.l. : Chainalysis, 2023.

59. **Ponemon Institute.** *2023 Cost of insider threats global report.* s.l. : DTEX, 2023.

60. **IBM.** *IBM X-Force Threat Intelligence Index 2024.* s.l. : IBM, 2024.

61. **Dawn Cappelli, Andrew P. Moore & Randall F. Trzeciak.** *The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud).* s.l. : Addison-Wesley Professional, 2012. ISBN9780321812575.

62. **Poremba, Sue. Verizon.com.** *[Internett] [Sitert: 4 4 2024.] https://www.verizon.com/business/resources/articles/s/the-risk-of-insider-threat-actors/.*

63. **National Cyber Security Centre UK.** *The near-term impact of AI on the cyber on the cyber threat.* London : NCSC, 2024.

64. **Malwarebytes.com.** *Big-game hunting (BGH).* [Internett] https://www.malwarebytes.com/glossary/big-game-hunting-bgh.