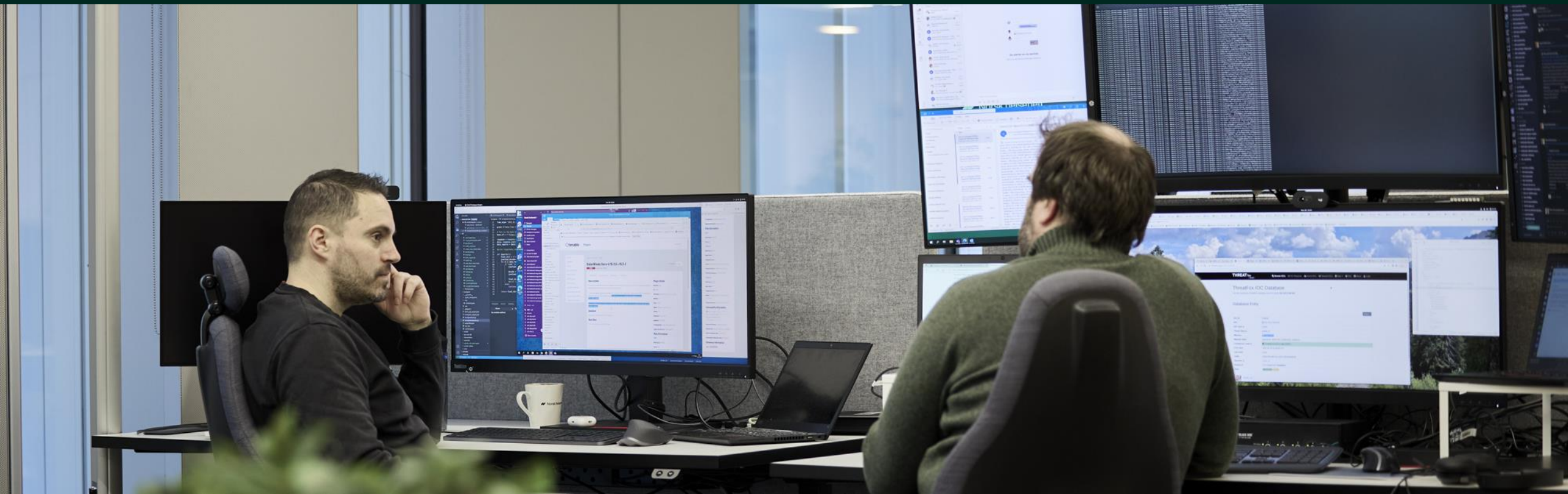
Norsk helsenett

HelseCERTs tilbakeblikk

2023, 1.tertial



Innhold

Forord

Situasjonsvurdering og anbefalte tiltak

Nytt fra HelseCERT

Hendelser siste periode

Anbefalinger*

Statistikk for deres virksomhet*

Statistikk for alle virksomheter i NBP

Funn fra inntrengingstester

* forutsetter tjenesten sikkerhetsskanning

Forord

Den sikkerhetspolitiske situasjonen i Europa har endret seg kraftig i løpet av det siste året. Vi ser økt etterretningstrussel, kraftig økt aktivitet fra hacktivister og en stadig større avstand til Russland. I Sikkerhetsfaglig råd skriver Nasjonal sikkerhetsmyndighet (NSM): «*…fremmede staters og trusselaktørers bruk av teknologi kan komme til å utvikle seg raskere enn åpne demokratiers evne til å beskytte seg…»* og *«Beredskap må bygges i fredstid, og nå må vi prioritere tiltak som sikrer et motstandsdyktig Norge*».

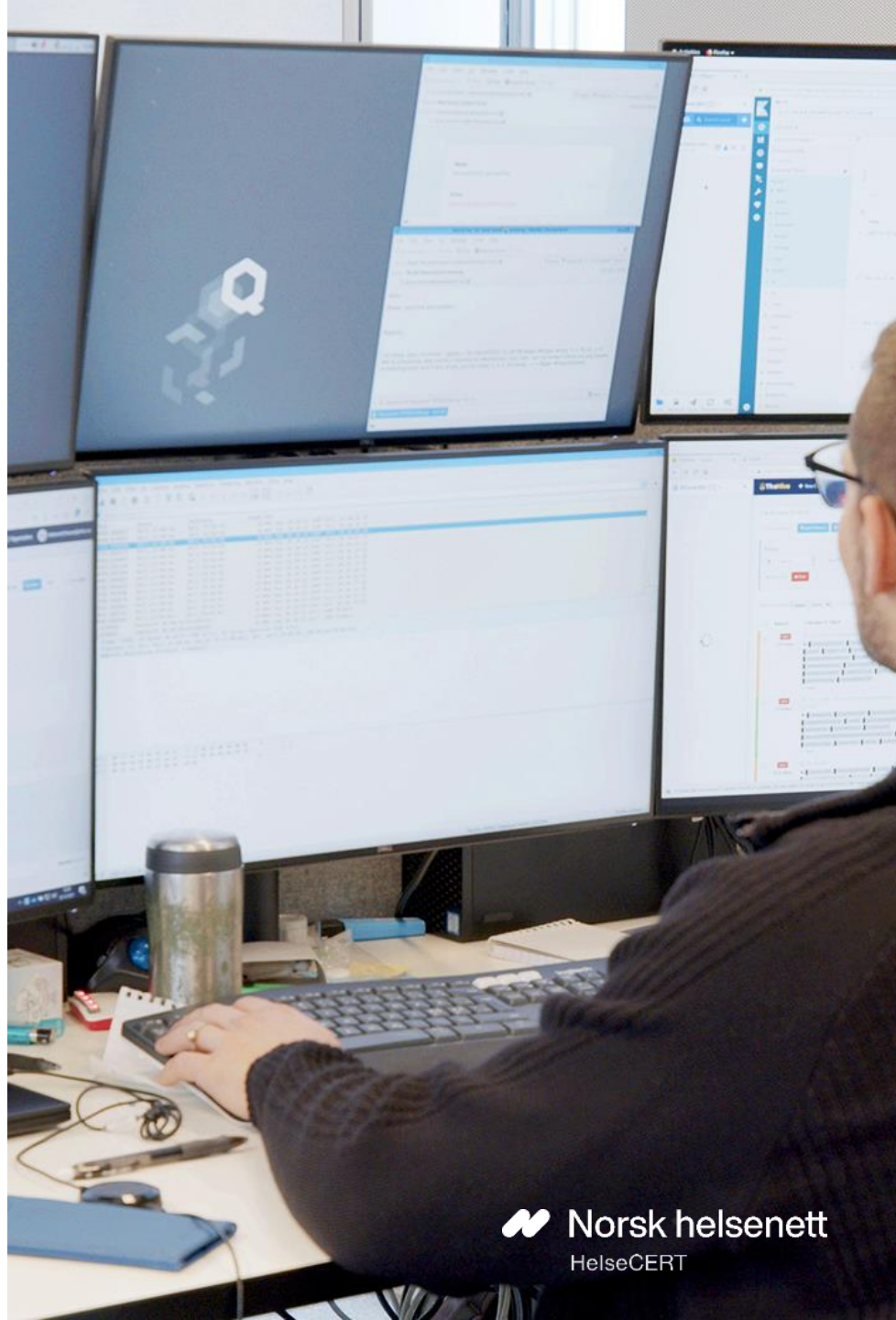
Mye er i endring. Det som i mindre grad har endret seg er hva som er smart å gjøre for å beskytte seg. God sikkerhet handler i stor grad om god og sikker drift. God drift inkluderer kontroll på hvilke tjenester man har, rutiner for oppdatering, fjerning av programvare og tjenester som ikke brukes, kontroll på tilgangsstyring, m.m.

Det finnes ikke en enkelt løsning som løser disse utfordringene for oss. De må løses systematisk over tid i felleskap mellom ledelse og de som drifter systemene. Dette underbygges av hva NSM skriver videre i Sikkerhetsfaglig råd: «*Virksomheter og befolkning har svært begrensede juridiske og praktiske muligheter til selv å påvirke en trusselaktør gjennom aktive tiltak. Deres innsats ligger i forebyggende og defensive sikkerhetstiltak…*».

På de neste sidene kommer vi med konkrete råd for forebyggende arbeid samt spesifikke anbefalinger for akkurat din virksomhet. Vi håper disse anbefalinger kan hjelpe dere i prioritering av det forebyggende arbeidet.

Sammen gjør vi helsesektoren sikrere!

Med hilsen
HelseCERT



Situasjonsvurderinger

- Det er meget sannsynlig at fremmede stater ser på helsesektoren som et mål for spionasje.
- Vi mener det er sannsynlig at norsk helsesektor vil treffes av angrep fra russiske statlige aktører som et ledd i det generelle etterretningsarbeidet til russiske etterretningstjenester.
- Vi mener det er meget sannsynlig at norsk helsesektor vil treffes av angrep fra organiserte kriminelle grupper.
- Vi mener det er meget sannsynlig at norsk helsesektor vil treffes av angrep fra hacktivister motivert av krigen i Ukraina. Eksempler på dette kan være tjenestenektangrep.

Oppdatert versjon av HelseCERTs situasjonsbilde er publisert på våre nettsider.

Anbefalte tiltak

1. Lukk alle sårbarheter medium og høyere som er rapportert i vår sårbarhetsoversikt.
2. Gå gjennom portskannrapporten vår og fjern unødvendige tjenester.
3. Sjekk at alle internetteksponerte tjenester med pålogging krever flerfaktor-autentisering.
4. Kjør HelseCERTs Hurtigtest for cybersikkerhet.
5. Blokker makroer i officedokumenter fra internett.
6. Innfør Microsofts ASR-regler.
7. Innfør applikasjonshvitelisting.
8. Se hovedfunn og anbefalinger fra våre inntrengingstester.

Nytt fra HelseCERT

Hurtigtest v3.0 er tilgjengelig

HelseCERT Hurtigtest er en automatisert sikkerhetstest som tar for seg de mest grunnleggende svakhetene våre pentestere normalt finner ute i sektoren. Versjon 3 inneholder nå blant annet en sjekk etter svakheter i Windows sertifikathåndtering. For mer informasjon se endringslogg. Testene som er inkludert i Hurtigtest er basert på erfaringer vi har gjort oss over mange år med sikkerhetstesting. Hurtigtest tilbys alle medlemmer i NBP. Ny versjon av Hurtigtest ble sluppet i løpet av 1. tertital.

Vi oppfordrer alle medlemmer til å kjøre Hurtigtest. Ønsker og innspill til nye features og forbedringer kan sendes til post@helsecert.no

Logging

For å effektivt kunne oppdage og håndtere hendelser er logging helt essensielt. Uten gode logger vil du praktisk talt være blind, både med tanke på å oppdage og håndtere hendelser. Vi har så langt i år kjørt en serie webinarer med fokus på logging og håper disse har vært til nytte.

Alle våre webinarer om logging, logganbefalinger og tips om hvordan komme i gang ligger tilgjengelig på helsecert.no

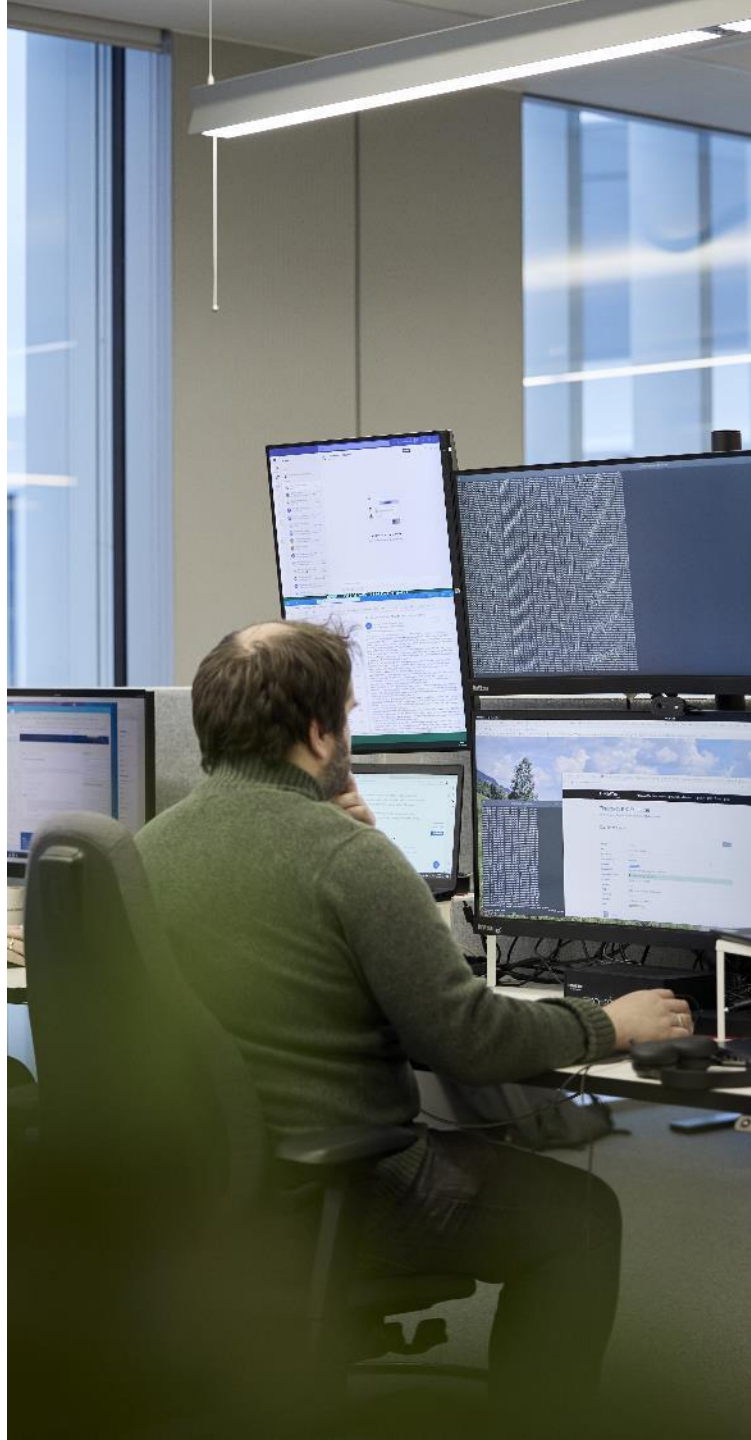
Sikkerhetsskanning

Sikkerhetsskanningen vår inkluderer, sårbarhetsskanning, portskanning og statusrapport for e-postsikkerhet (DMARC, DKIM, SPF, m.m.)

Vi jobber løpende med videreutvikling og oppdatering av vår sikkerhetsskanning. Vi har implementert flere kilder i vår datainnsamling som nå er inkludert i vår automatiserte varsling til dere.

Det viktigste bidraget vi ønsker fra dere i NBP er:

- Følg opp sårbarheter vi varsler om.
- Bruk portskannrapporten for å redusere angrepsflate.
- Meld inn endringer i IP-adresser og domener dere eier. Meld inn IPv6-adresser.
- Ta kontakt om dere oppdager feil. post@helsecert.no



Hendelser

Norsk helsenett
HelseCERT

To utvalgte hendelser hvor vi har vært involvert i håndtering:

Uautorisert tilgang til VPN løsning: Svakt passord på en VPN-løsning gjorde at angriper lyktes å logge inn i et lab-miljø. Angriper koblet opp en VPN-tunell over en periode på ca 5 minutter. Via denne tunellen hadde de potensiell tilgang til flere systemer. Analyse av loggdata tyder ikke på at angriper har gjort mere enn å bekrefte tilgang. Vi antar at angriper planla å komme tilbake på et senere tidspunkt.

Kompromittering gjennom underleverandør: Angriper fikk tilgang til brukernavn og passord hos en underleverandør av flere NBP-medlemmer. Dette ga tilgang inn i flere virksomheter. Raskt mitigerende arbeid gjorde at angriper ble stoppet underveis og forhindret at hendelsen fikk større konsekvenser.

Anbefaling: Begge hendelsene ovenfor ville vært avverget ved bruk av flerfaktorautentisering.

Verdikjedeangrep

I mars ble det oppdaget at VOIP-programvare fra selskapet 3CX var blitt kompromittert og brukt til å igjen angripe en rekke kryptovalutaselskap som brukte 3CX for kommunikasjon.

Sikkerhetsselskapet Mandiant ble leid inn av 3CX for å undersøke, og oppdaget at 3CX var selv var rammet av et leverandørkjedeangrep, noe som gjør dette til første (kjente) tilfelle av et to-stegs verdikjedeangrep. Basert på Mandiant undersøkelser var det angriperne en Nord-Koreansk gruppe.

Vi forventer å se flere verdikjedeangrep framover og framhever viktigheten av godt dybdeforsvar for å beskytte seg mot slike angrep. Se nettsiden vår for anbefalte herdetiltak.

Tjenestenektangrep

I slutten av januar ble Norsk helsenetts felles nettløsning for spesialisthelsetjenesten (FNSP) rammet av tjenestenektangrep. Angrepene førte til kortvarig ustabilitet på nettsidene, men ut over det har hendelsene ikke ført til negative konsekvenser for helsetjenesten. Vi observerte flere runder med angrepsforsøk og det ble fortløpende gjort små justeringer av tiltak for å motstå angrepene og minimere nedetid.

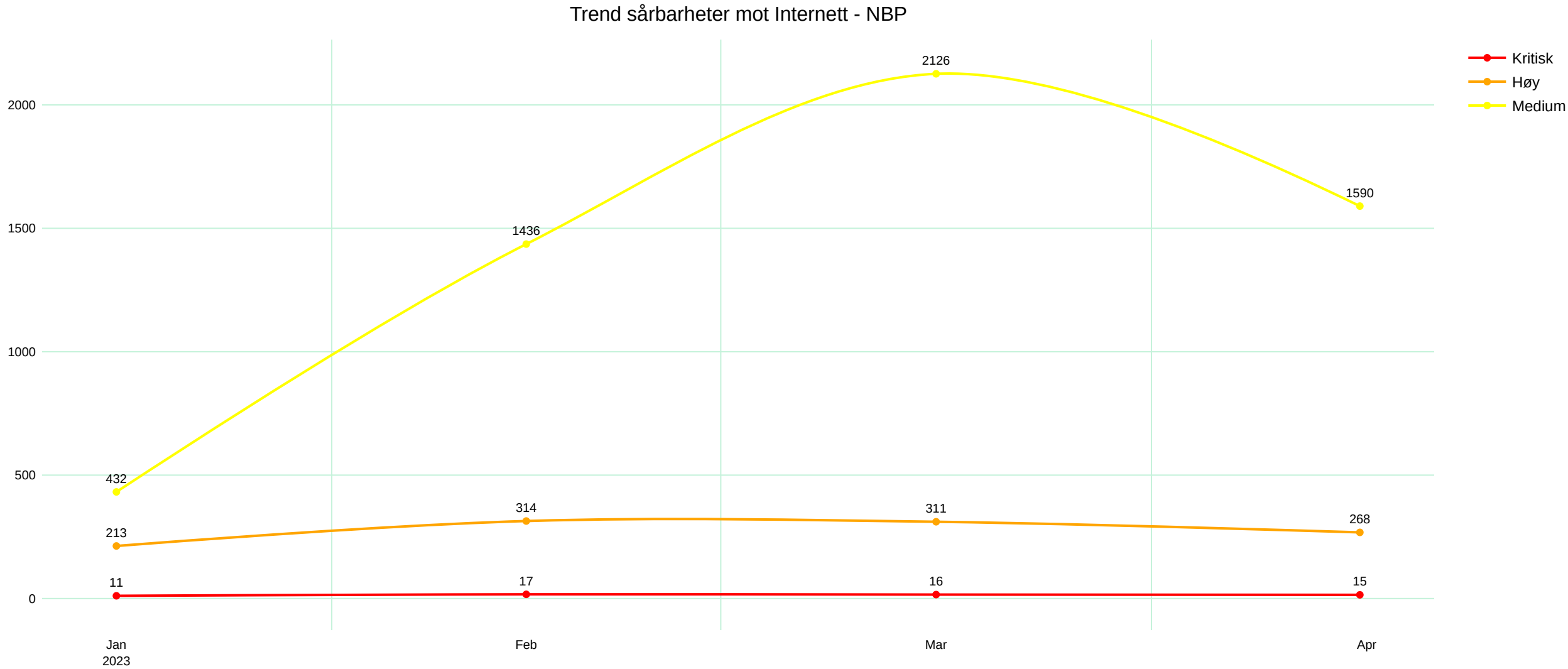
Formålet med slike tjenestenektangrep er å påvirke stabilitet og tilgjengelighet på de sidene som blir rammet. Denne type angrep innebærer at det sendes et stort antall forespørsler til en nettside slik at den ikke har kapasitet til å svare. Dermed oppleves nettsiden som utilgjengelig.

Etter utbruddet av krigen i Ukraina har denne typen angrep mot land som støtter Ukraina blitt vanlig og vi ser ukentlig denne typen angrep i Europa. Dette er andre gangen i løpet av det siste året vi registrerer angrep mot flere norske nettsider samtidig. Det forrige var i fjor sommer. Angrepene har så langt fått små konsekvenser og det er liten risiko for at interne systemer blir rammet av denne typen angrep.

Se vår nettside for mer informasjon om tjenestenektangrep og tips om hvordan man bør beskytte seg.

Trend sårbarheter mot Internett – NBP
Økning av sårbarheter i februar/mars har sammenheng med at flere tjenester blir skannet.

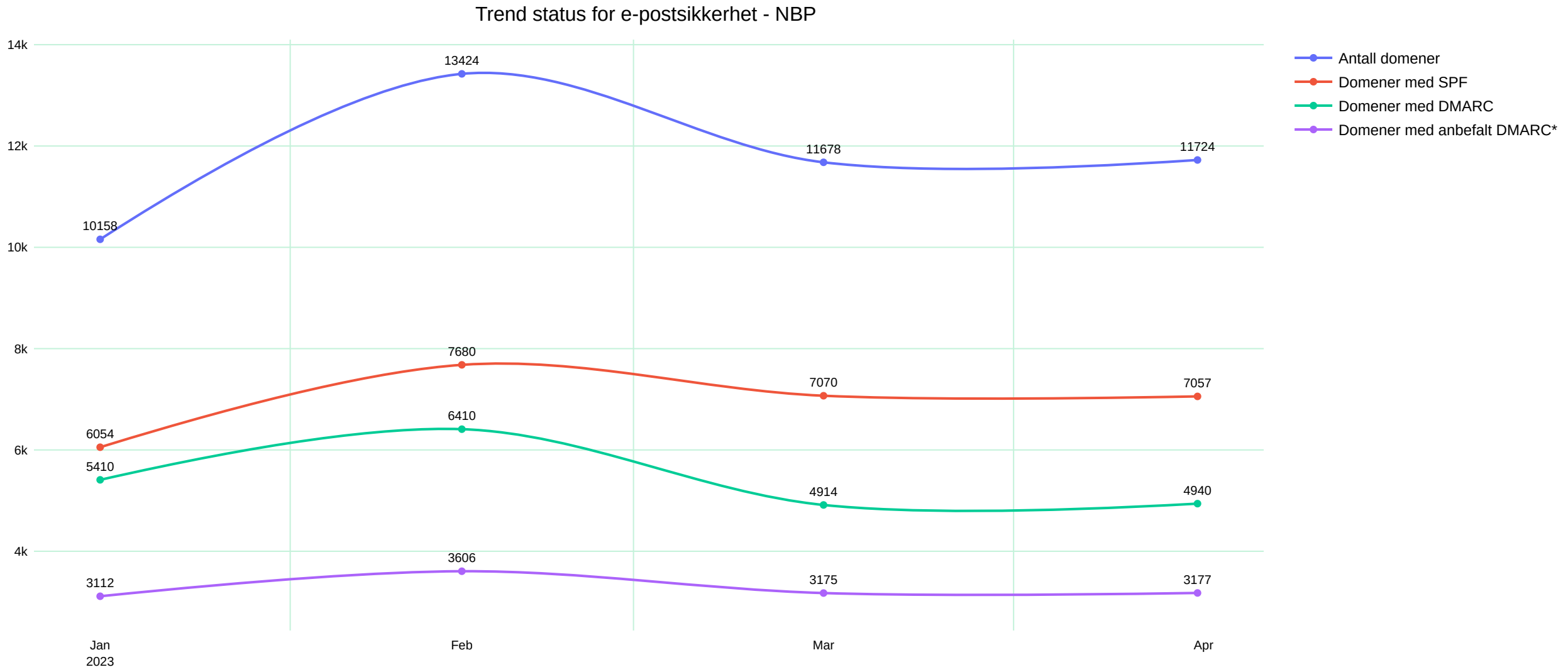
Norsk helsenett
HelseCERT



Trend sårbarheter for e-postsikkerhet – NBP

Vi ser liten utvikling i bruk av DMARC så vi oppfordrer alle til å bruke egen oversikt for e-postsikkerhet i denne rapporten og følg: https://www.nhn.no/om-oss/Personvern-og-informasjonssikkerhet/helsecert/anbefalte-sikkerhetstiltak/e-postsikring/dmarc til å implementere DMARC.

Norsk helsenett
HelseCERT



Hovedfunn inntrengingstester

1

Svake passord
Passordpolicy er generelt blitt bedre i sektoren men vi finner fortsatt brukere med svake passord. Ofte er dette brukere som sjelden eller aldri logger inn og dermed ikke har oppdatert passord etter at ny policy ble innført. Kontoer med svake passord utgjøre en høy risiko.

Anbefaling: Følg vår passordpolicy på helsecert.no. Benytt Hurtigtest for å avdekke svakheter. Ta i bruk verktøy som kontrollerer passordkvalitet.

2

Interne systemer som ikke følger beste praksis
Vår erfaring er at internt utviklede systemer har mindre fokus på sikkerhet. Dette gir seg utslag i mangelfull tilgangsstyring, kryptografisk svikt og generelt usikkert design.

Anbefaling: Sørg for at interne utviklingsprosesser følger beste praksis. Avvikle programvare hvor det ikke lenger gjøres utvikling og vedlikehold av kildekoden.

3

Sensitiv informasjon på delte filområder
Vi finner ofte passord og annen sensitiv informasjon i filer på delte filområder. Konfigurasjonsfiler, administrasjonsskript og backupfiler er gjengangere.

Anbefaling: Gjør en gjennomgang av delte filområder. Vurder innhold og hvem som trenger tilgang. Etabler løsning for sikker lagring av passord.

4

Dårlig sikring av interne systemer
Telefoner, printere, byggtekniske og medisinskteknisk utstyr har oftere manglende tilgangsstyring eller fabrikkpassord som er lett å finne for en angriper. Dette åpner for muligheten for å forstyrre driften av virksomheten og gir angriper muligheten til å etablere fotfeste.

Anbefaling: Skift fabrikkpassord på nytt utstyr før det kobles til nettverk. Sett sterke administratorpassord. Vurder om slikt utstyr bør segmenteres i egne nett.

5

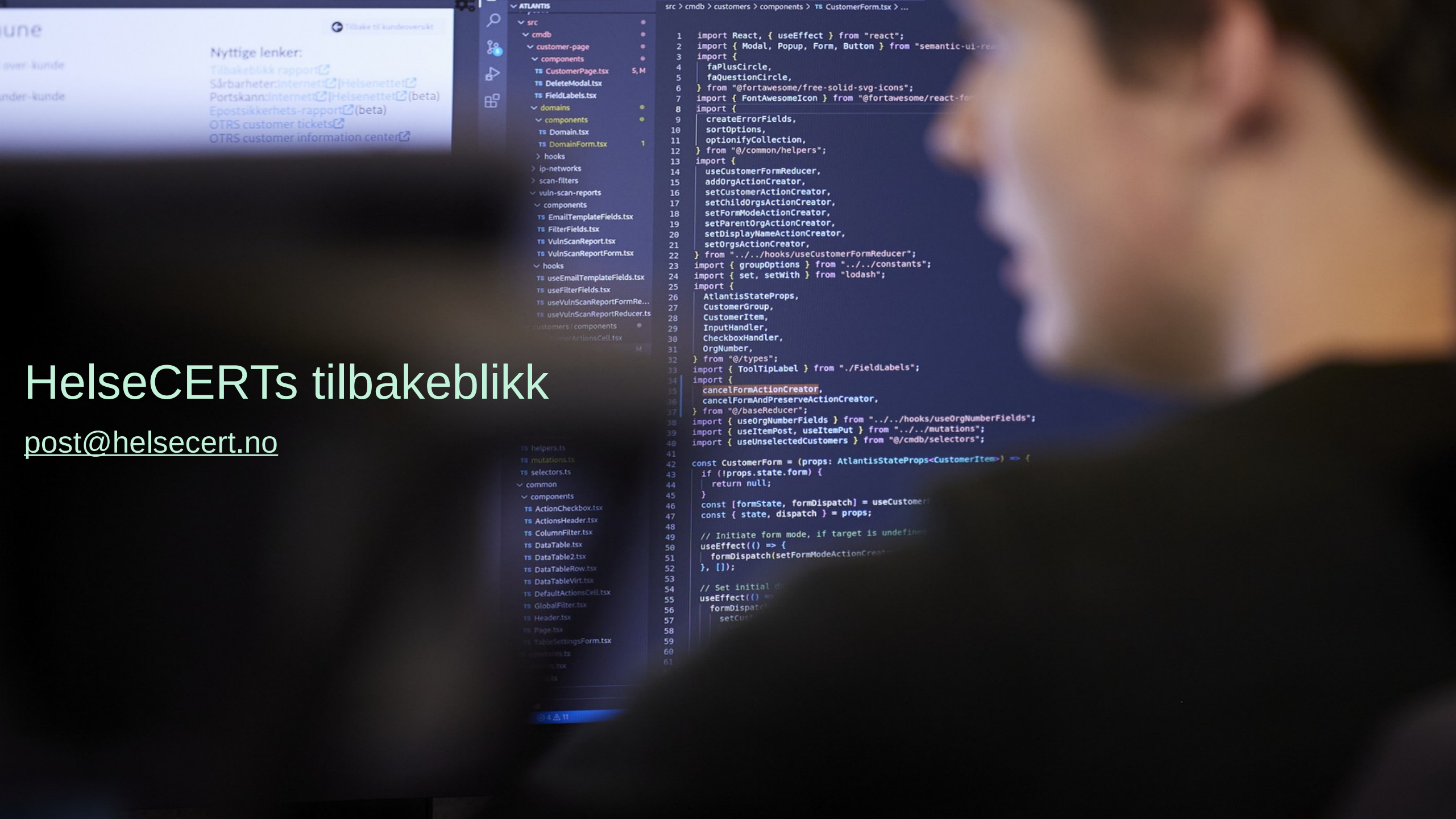
Svak sikring av terminalserver
Sikringstiltak av terminalserver er generelt dårligere enn på vanlige klienter. Stor nettverkstilgang, manglende applikasjonshvitelisting og brede tilganger til delte filområder gjør disse maskinene attraktive for en angriper.

Anbefaling: Implementer applikasjonshvitelisting og generell herding.

6

Feilkonfigurert tilgangsstyring for sertifikater (AD CS)
Mangelfull tilgangsstyring av hvem som kan utstede sertifikater i Active Directory kan utnyttes til å eskalere rettigheter.

Anbefaling: Blokker muligheten for utstedelse av sertifikater på vegne av vilkårlige brukere.



HelseCERTs tilbakeblikk

post@helsecert.no