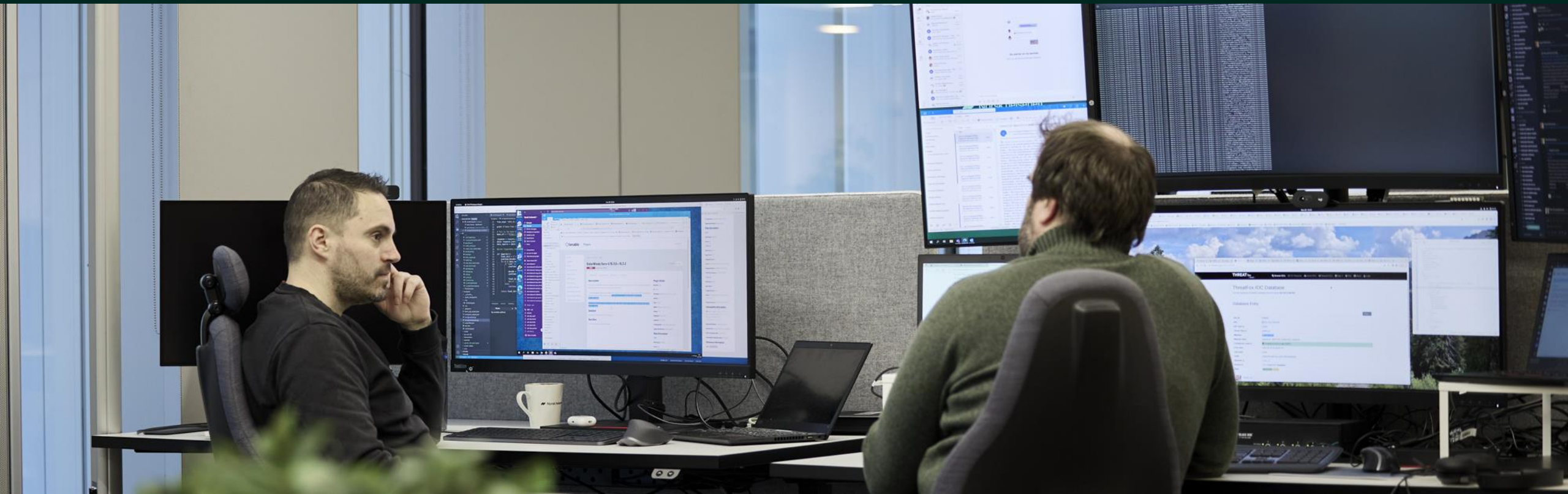
Norsk helsenett

HelseCERTs tilbakeblikk

Nasjonalt beskyttelsesprogram

2023, 2.tertial



Innhold

Forord

Sommeren har vært preget av et uvanlig høyt aktivitetsnivå i HelseCERT. Det har vært flere hendelser med alvorlige sårbarheter og vi har bistått en rekke virksomheter med kompromitteringer. Vi har hatt en aktiv koordinerende rolle mellom SRMer, NCSC og internasjonale samarbeidspartnere i forbindelse med flere av hendelsene.

Vi ser at informasjon vi har delt med våre nasjonale og internasjonale samarbeidspartnere har gitt oss svært verdifull informasjon tilbake som har bidratt til at vi har oppdaget flere kompromitterte systemer i helsesektoren. Dette viser viktigheten av å dele informasjon om hendelser og sårbarheter.

For den enkelte virksomhet handler godt sikkerhetsarbeid mye om å **forebygge** og **oppdage** sikkerhetshendelser:

- **Forebyggende** sikkerhetsarbeid utføres av absolutt alle ansatte. Litt hver dag. Det handler om vedlikehold av IKT-infrastruktur og ansatte som tar kloke valg i hverdagen gjennom bevissthet og tilstrekkelig kunnskap. God risikostyring basert på god trusselforståelse støtter oppunder dette.
- Evnen til å **oppdage** hendelser krever en kombinasjon av tilstrekkelig logg-grunnlag fra systemer og tjenester, alarmering på dette og ansatte som følger med på alarmene. I tillegg er en kultur hvor avvik rapporteres utrolig viktig.

Med hilsen
HelseCERT - Sammen gjør vi helsesektoren sikrere!

Nytt fra HelseCERT

Sikkerhetsfestivalen på Lillehammer

HelseCERT var godt representert på sikkerhetsfestivalen på Lillehammer. I tillegg til tre deltakere holdt Jørgen Bøhnsdalen fra HelseCERT to innlegg i løpet av festivalen. Ett av disse ble presentert som webinar 8. September - "Utpressing neste"

Nasjonalt beskyttelsesprogram

Oppdatert versjon av HelseCERTs situasjonsbilde er publisert og tilgjengelig på våre nettsider.

Gjennom nasjonalt beskyttelsesprogram for helse- og omsorgssektoren tilbyr vi en rekke tjenester for virksomheter i sektoren. Formålet med tjenestene er å bidra til å heve sikkerheten i sektoren.

For en komplett oversikt over hvilke tjenester vil tilbyr og hvordan dere tar de i bruk, se helsecert.no.

Hendelseshåndtering

Vi ønsker å bli informert om hendelser dere i sektoren har, også i tilfeller der dere ikke har behov for bistand.

Vi bistår dere kostnadsfritt i hendelseshåndtering. Type og mengde bistand er avhengig av tilgjengelig kapasitet.

God oversikt over hva som skjer i sektoren gjør oss i stand til å rette vårt eget arbeid til der det har mest effekt. Det gjør oss også i stand til å dele et mest mulig komplett og nyttig bilde til alle i sektoren.

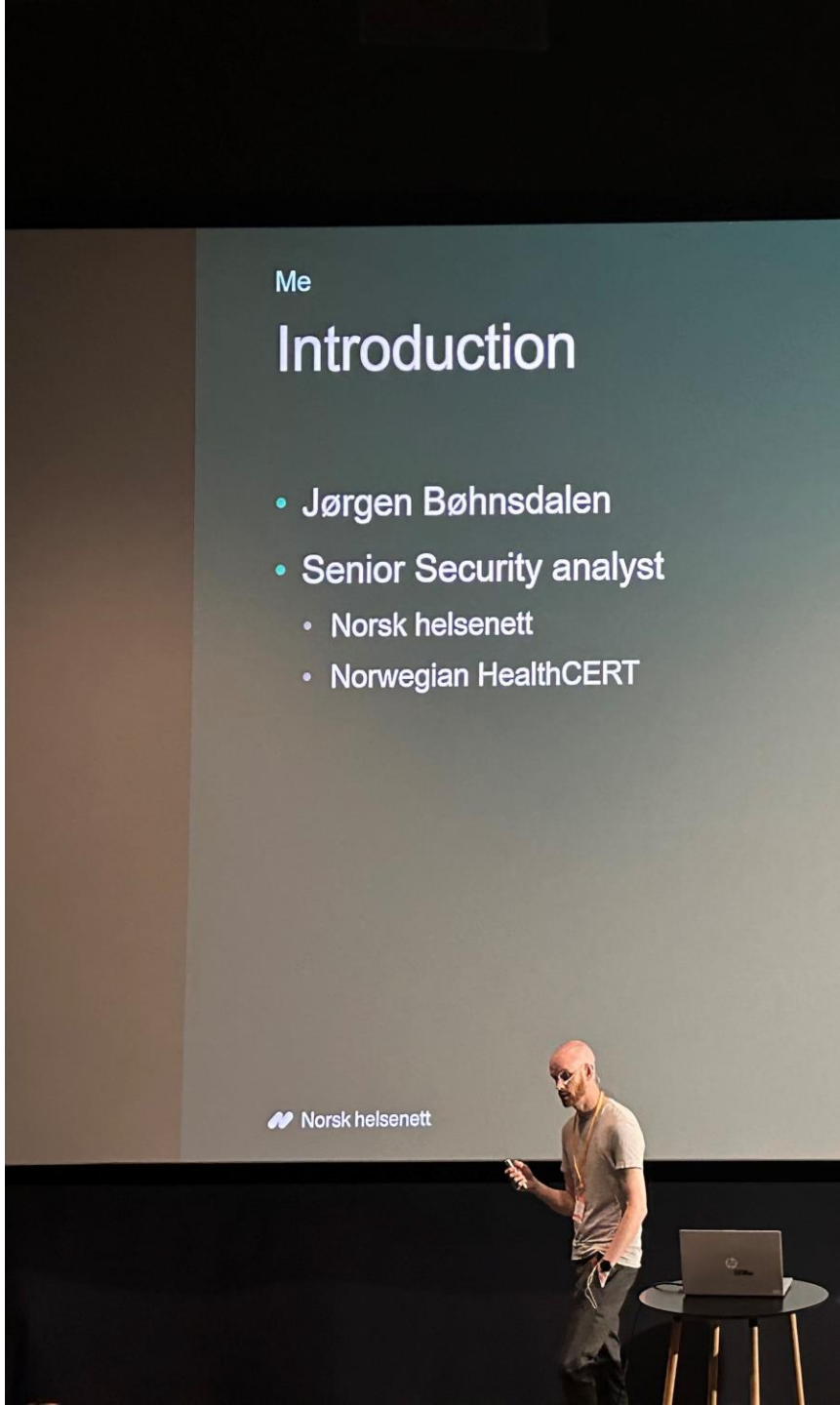
Dere kan kontakte oss på e-post eller telefon:
post@helsecert.no / +47 24 20 00 00

Webinarer

Vi har tidligere i kjørt en serie webinarer med fokus på logging. Logging er viktig både for å oppdage og håndtere hendelser.

De neste webinarene fra oss vil gå igjennom noen utvalgte hendelser vi har jobbet med, samt sette fokus på hendelseshåndtering.

Informasjon om våre kommende webinarer og opptak av tidligere webinarer finner dere på vår nettside.



Hendelser

Utpressing neste

En virksomhet i sektoren ble utsatt for et dataangrep via en sårbar internetteksponert løsning. Det fantes både utnyttelseskode for - og oppdatering som lukket - denne sårbarheten. Angriper lyktes med å oppnå tilgang til flere andre systemer og ble til slutt domeneadministrator. Som domeneadministrator har de hatt tilgang til flere systemer, men virksomhetens sikkerhetsløsning (EDR) isolerte systemer straks eksfiltrasjon av data ble forsøkt. Deretter ble hendelseshåndteringen startet. EDR og hendelseshåndtering forhindret at helserelaterte systemer ble berørt.

Hendelseshåndteringen har vært omfattende, og med mye analysearbeid for å få oversikt over hendelsesforløp. Analysene viser at minst tre ulike angripere har vært inne hos virksomheten. Hendelsen førte til noe nedetid men ikke hatt større konsekvenser for helsetjenesten.

Blant angriperne som har vært inne på systemene vet vi at det har vært minst en utpressingsaktør, i tillegg til en gruppe (Mint Sandstorm / Tunnelvision) som i åpne kilder knyttes til Iran. Angriper som fikk mest tilgang forsøkte å kjøre bakdøren BADHATCH på alle maskiner de logget seg på. Vår vurdering rundt alle disse angrepene er at de gikk spesifikt mot den aktuelle løsningen/sårbarheten, og at de ikke var ute etter den spesifikke virksomheten i seg selv.

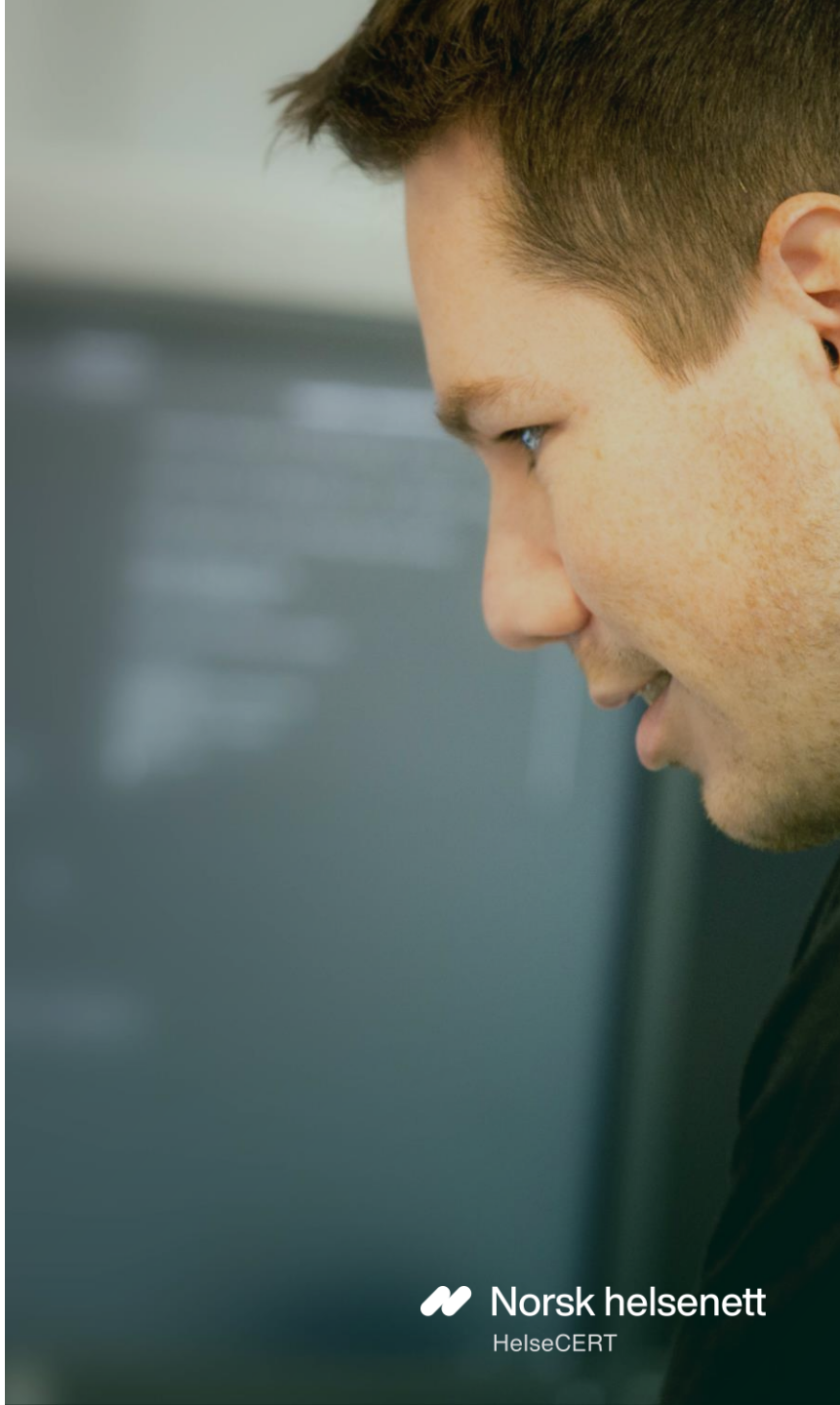
Denne hendelsen ble presentert i et webinar 8. september 2023.

Tjenestenektangrep

Vi ser fortsatt at ulike pro-russiske hacktivister utfører tjenestenektangrep mot land som støtter Ukraina, norske nettsider rammes også jevnlig. Hendelsene får i all hovedsak små konsekvenser og merkes i liten grad av brukerne av tjenestene.

Vi forventer at norske nettsider vil bli utsatt for tjenestenektangrep også utover høsten.

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



Hendelser

Nulldagssårbarhet i Citrix ADC

Overordnet

- **18. juli**: Citrix publiserer varsel om kritisk sårbarhet (CVE-2023-3519), samt oppdatering som lukker sårbarheten. Sårbarheten har da allerede vært utnyttet i målrettede angrep.
- **20. juli**: Masseutnyttelse av sårbarhet starter, rundt 2000 webshell plantes verden over.
- **3. august**: Kode for utnyttelse av sårbarheten blir offentlig tilgjengelig
- **20. august**: Skadevaren BADHATCH blir observert kjørt på maskiner knyttet til Citrix ADC-instanser med webshell plantet gjennom utnyttelse av CVE-2023-3519

Håndtering

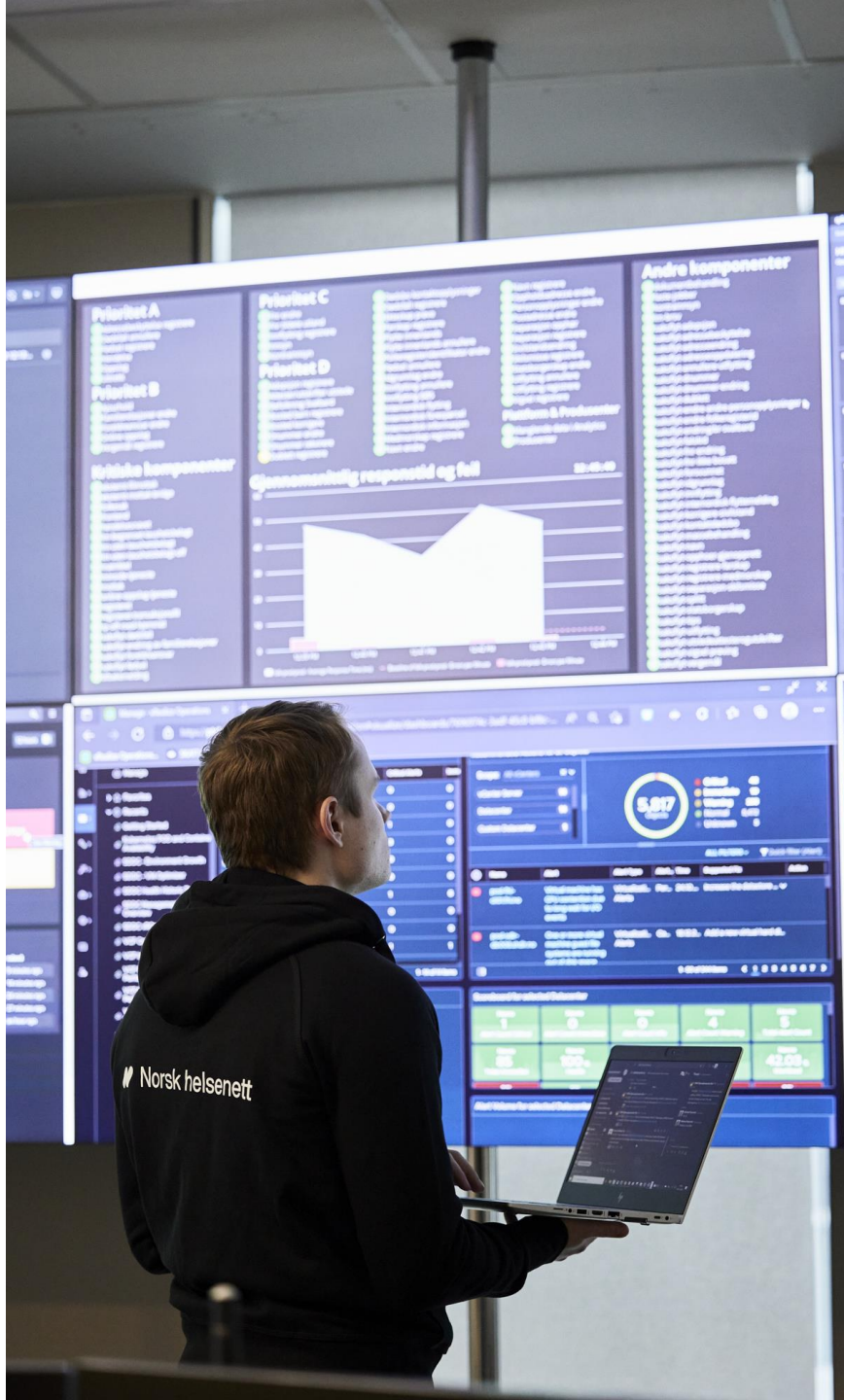
Gjennom skanning av medlemmer i Nasjonalt beskyttelsesprogram for helse- og omsorgssektoren (NBP) ble det identifisert Citrix Netscaler ADC-instanser eksponert på cirka 220 IP-er, fordelt på 85 virksomheter. Vi sendte ut et fellesvarsel om sårbarheten, og fulgte deretter opp de som fortsatt var sårbare med direktevarsler. De som ikke responderte på e-postvarsel, ble oppringt.

Av de 85 virksomhetene ble det avdekket at 10 hadde blitt kompromittert med et webshell. Webshellene ble plassert hhv. 20., 21. og 31. Juli, og var lagt slik at de fortsatt lå på systemet selv etter oppdatering.

Virksomhetene som ble kompromittert var 6 kommuner, 2 driftsleverandører, 1 fylkeskommune og 1 annen virksomhet. Vi bisto med hendelseshåndtering hos alle virksomhetene, og alle tilfeller vi kjenner til er ryddet opp i. Vi er ikke kjent med omfattende kompromittering eller konsekvenser hos noen av virksomhetene som følge av webshellene. Nå har vi begynt å fått meldinger om at ikke-ryddede webshell begynner å bli tatt i bruk for påfølgende operasjoner.

Vi har gjennom hendelsen hatt stort fokus på informasjonsdeling med sektor og samarbeidspartnere, både nasjonalt og internasjonalt. Arbeidet har blant annet resultert i en blogpost fra Shadowserver. Vi ser at en rekke samarbeidspartnere og leverandører har brukt informasjon vi har delt for å avdekke kompromitterte systemer.

Hendelsen har, så langt vi kjenner til, ikke fått konsekvenser for helsetjenesten.



Trend sårbarheter mot Internett – NBP

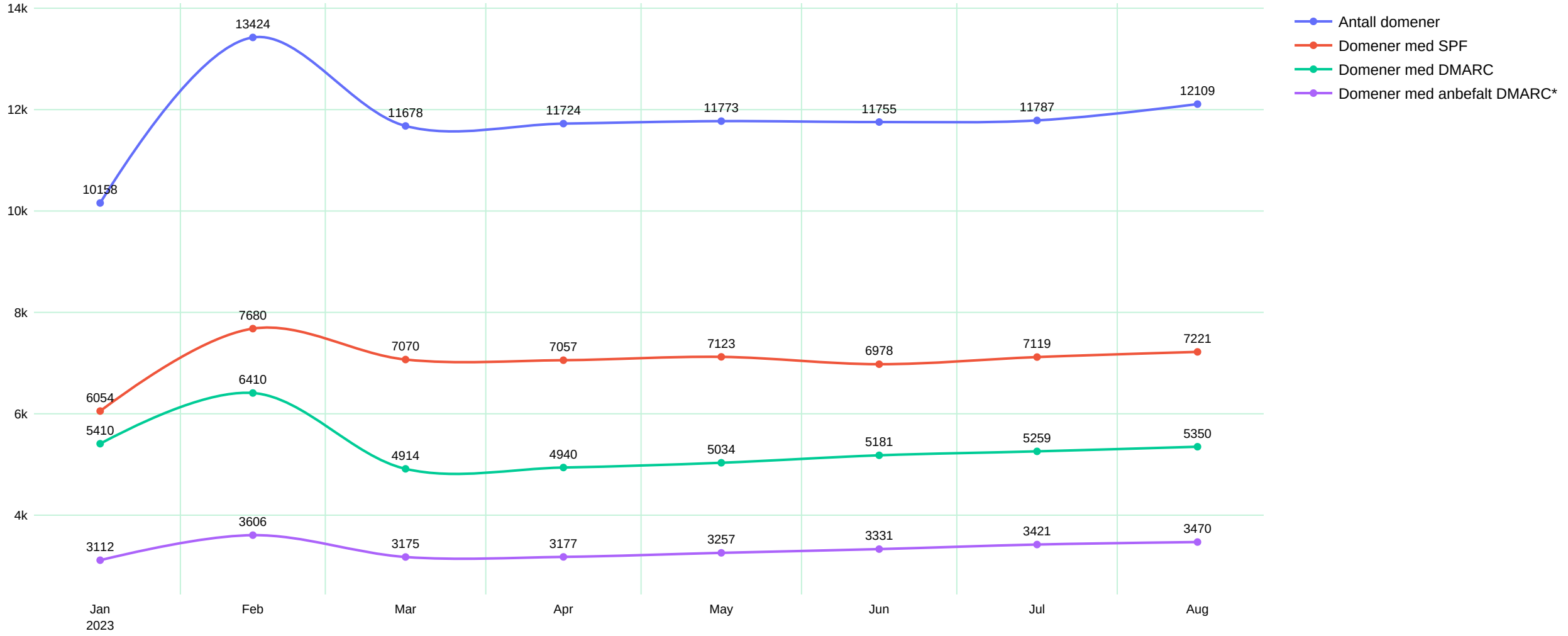
Norsk helsenett
HelseCERT

Økning av sårbarheter i februar/mars har sammenheng med at flere underdomener automatisk blir identifisert og skannet.
Reduksjonen av sårbarheter i april/mai er i hovedsak grunnet utfiltrering av falske positiver mot WAF-tjenester som Imperva, Cloudflare og Fastly.
Økningen vi ser i august skyldes en kombinasjon av flere ting. Vi skanner flere medlemmer/systemer samtidig som vi bruker flere kilder for å finne sårbarheter, samt forbedring i deteksjon for sårbarheter i PHP

Trend status for e-postsikkerhet – NBP

Norsk helsenett
HelseCERT

Vi ser ingen reell utvikling i bruk av DMARC i helsesektoren i løpet av siste tertial. 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. Bruk oss i HelseCERT om dere har spørsmål. post@helsecert.no



Tilbakeblikk 2. tertial 2023

Erfaringer fra 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

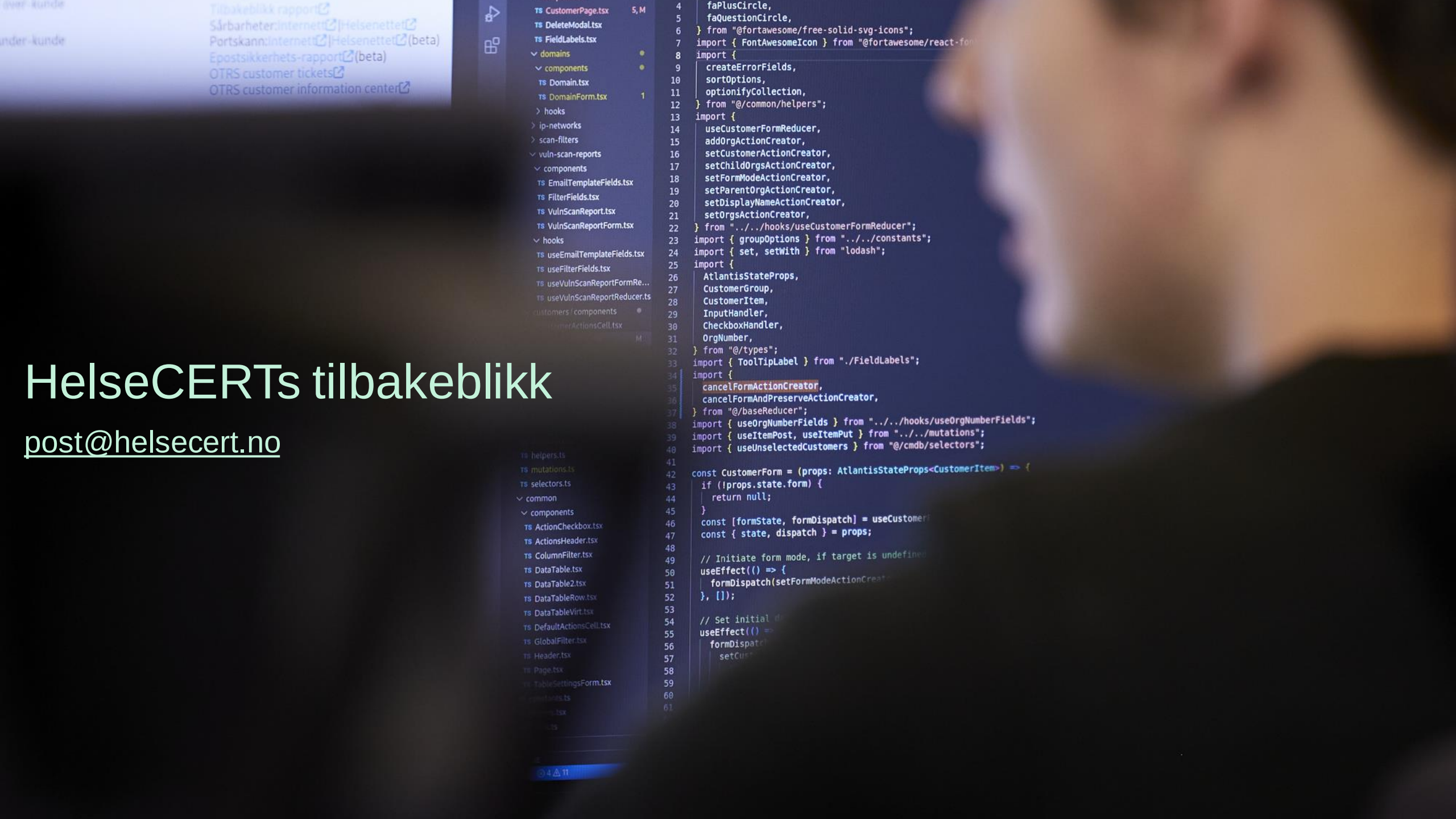
Feilkonfigurert tilgangsstyring for sertifikater (AD CS)
Mangelfull tilgangsstyring av hvem som kan utstede sertifikater i Active Directory kan utnyttes til å eskalere rettigheter.

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

Trusselvurdering

- 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 statlige eller stats-sponsede aktører som et ledd i det generelle arbeidet til statlige 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.



HelseCERTs tilbakeblikk

post@helsecert.no