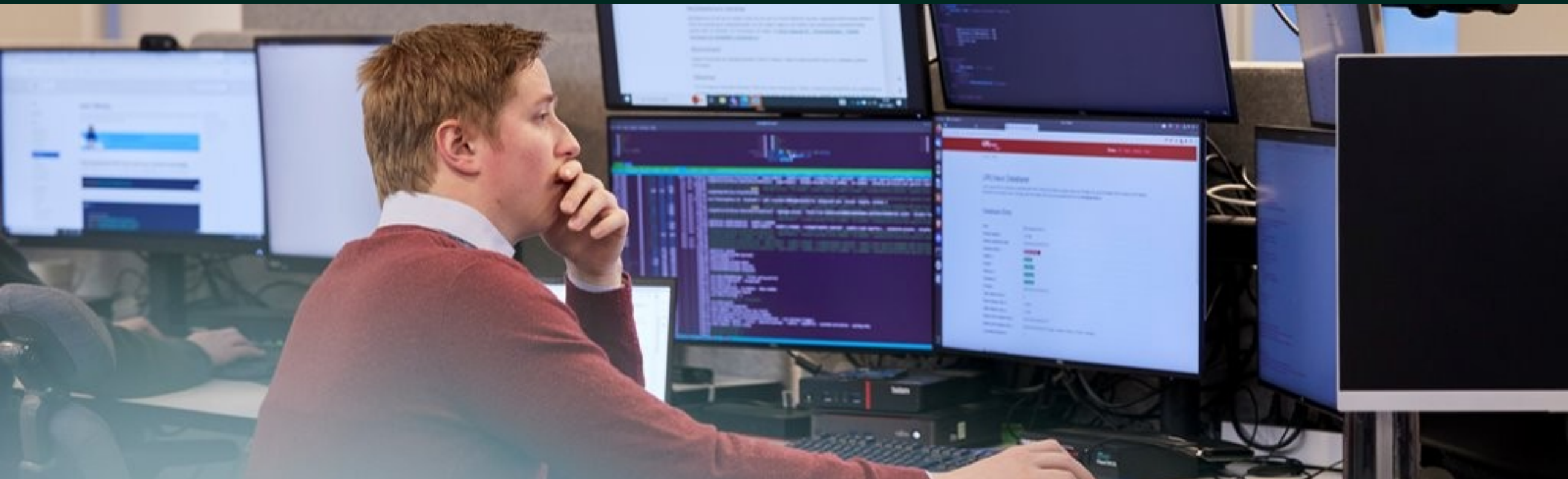
Norsk helsenett

HelseCERT | KommuneCERT
Tilbakeblikk 3. tertial 2023



Innhold

Forord

Nytt fra Helse- og KommuneCERT

Statistikk for varsler

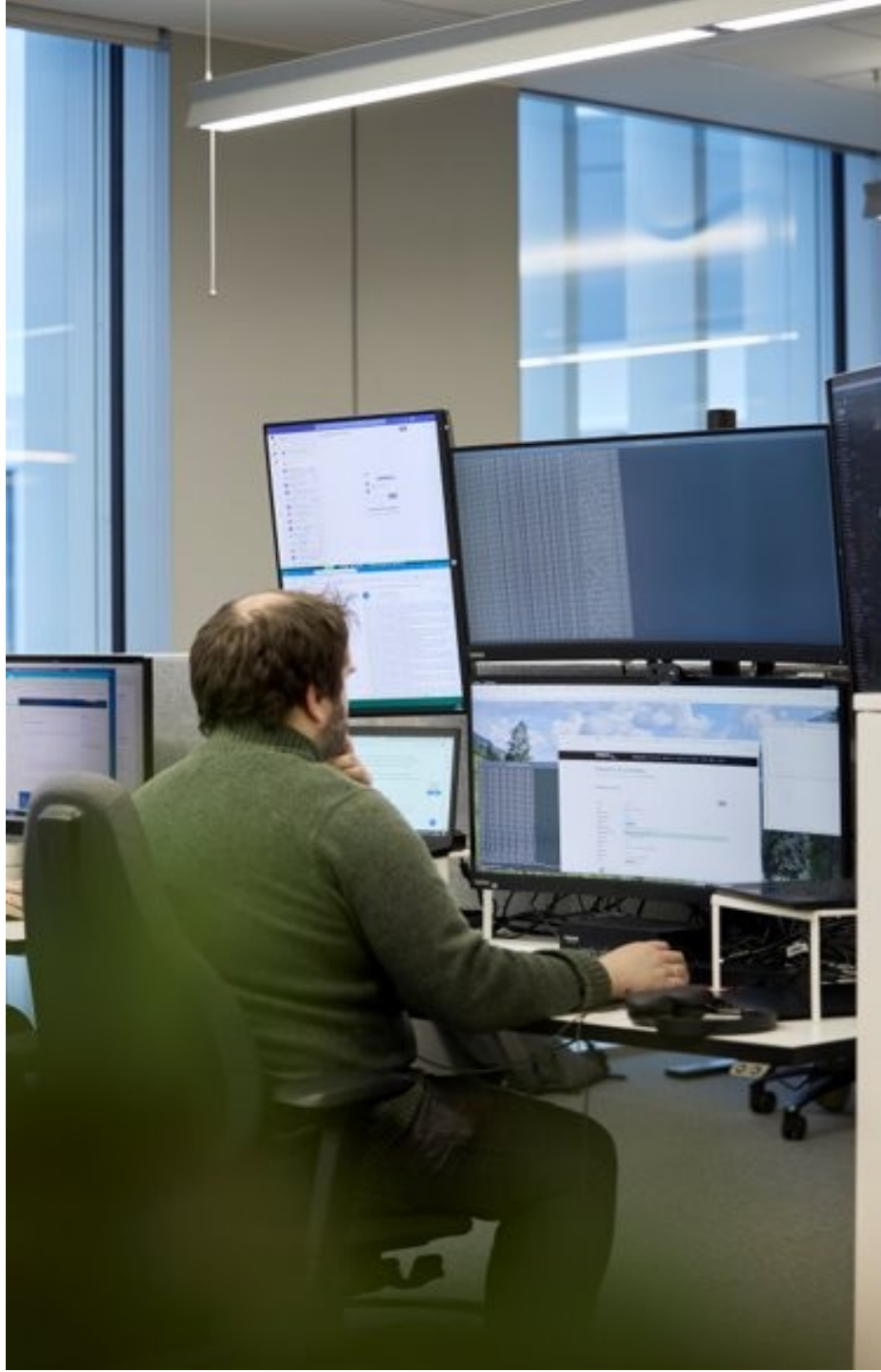
Trend sårbarheter mot Internett – NBP

Trend status for e-postsikkerhet – NBP

Hendelser og sårbarheter

Erfaringer fra inntrengingstester

Trusselvurdering



Forord

Hei og godt nytt år!

Året vi har lagt bak oss har for oss vært preget av hendelseshåndtering og et stort antall nye sårbarheter. Vi ser en økning i utnyttelse av sårbarheter, både før og etter at de blir offentlig kjent. Tiden fra en sårbarhet blir kjent til den utnyttes i store angrepsbølger er ofte svært kort. På slutten av året har vi sett en kraftig økning i phishingkampanjer som omgår multifaktorautentisering (MFA), noe som bekymrer oss da mange ikke har implementert phishingresistent autentisering. Vi forventer at disse trendene blir med oss i det kommende året.

I tiden fram til sommeren ønsker vi å teste ut et nytt konsept: Månedens tema. For hver måned vil vi velge ut et tema som vi kommer til å følge opp ekstra godt mot alle dere som er medlemmer i Nasjonalt beskyttelsesprogram (NBP). Vi håper på god oppslutning og aktiv deltakelse fra dere alle. Fokus i januar er at flest mulig av dere skal laste ned og kjøre vår Hurtigtest. Hvis alle medlemmer i NBP gjør dette og utbedrer funn så vil vi få en sikrere helse- og kommunesektor og sammen klare å øke vår felles digitale motstandskraft.

24. november i fjor fikk vi oppdrag om å etablere KommuneCERT i tilknytting til HelseCERT. Gjennom dette oppdraget skal vi jobbe med å øke motstandskraften i kommunesektoren gjennom å bidra til å forebygge, oppdage og håndtere digitale angrep. Vi er glade og ydmyke for at regjeringen og departementene har gitt dette oppdraget til oss og at de ønsker å bygge videre på kompetansen, erfaringene og tjenestene vi har bygget opp i HelseCERT. Det er hyggelig å bli vist tillit, og bra at kommuner og fylkeskommuner nå får et definert senter å kontakte ved hendelser. Vi ser fram til å jobbe enda tettere med dere i kommunesektoren i tiden framover.

Med hilsen
HelseCERT | KommuneCERT
- sammen gjør vi Norge sikrere!

Nytt fra Helse- og KommuneCERT

Ny versjon av Hurtigtest

Versjon 4.0 av Hurtigtest ble sluppet 5. januar. Hurtigtest er en automatisert sikkerhetstest som tar for seg de mest grunnleggende svakhetene våre pentestere normalt finner ute hos virksomheter. Utviklingen og testene som er inkludert er basert på erfaringer vi har gjort oss over mange år med sikkerhetstesting og tilbys alle medlemmer i NBP.

Nytt i versjon 4 er blant annet funksjonalitet for å avdekke sensitiv informasjon som ligger på delte filområder.

Last ned hurtigtest fra vår nettside.

Nasjonalt beskyttelsesprogram

Oppdatert versjon av vårt 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.

KommuneCERT

HelseCERT har blitt utpekt til å være offisielt sektorvis responsmiljø for kommunesektoren og fått i oppdrag å etablere KommuneCERT. I november kunngjorde regjeringen at de ønsker å etablere et digitalt sikkerhetsmiljø for å styrke kommunenes vern mot digitale trusler. Oppdraget inkluderer også fylkeskommunene. Regjeringen ønsker å bygge videre på miljøet som finnes i HelseCERT. Pressemelding fra regjeringen er tilgjengelig på regjeringen sine nettsider.

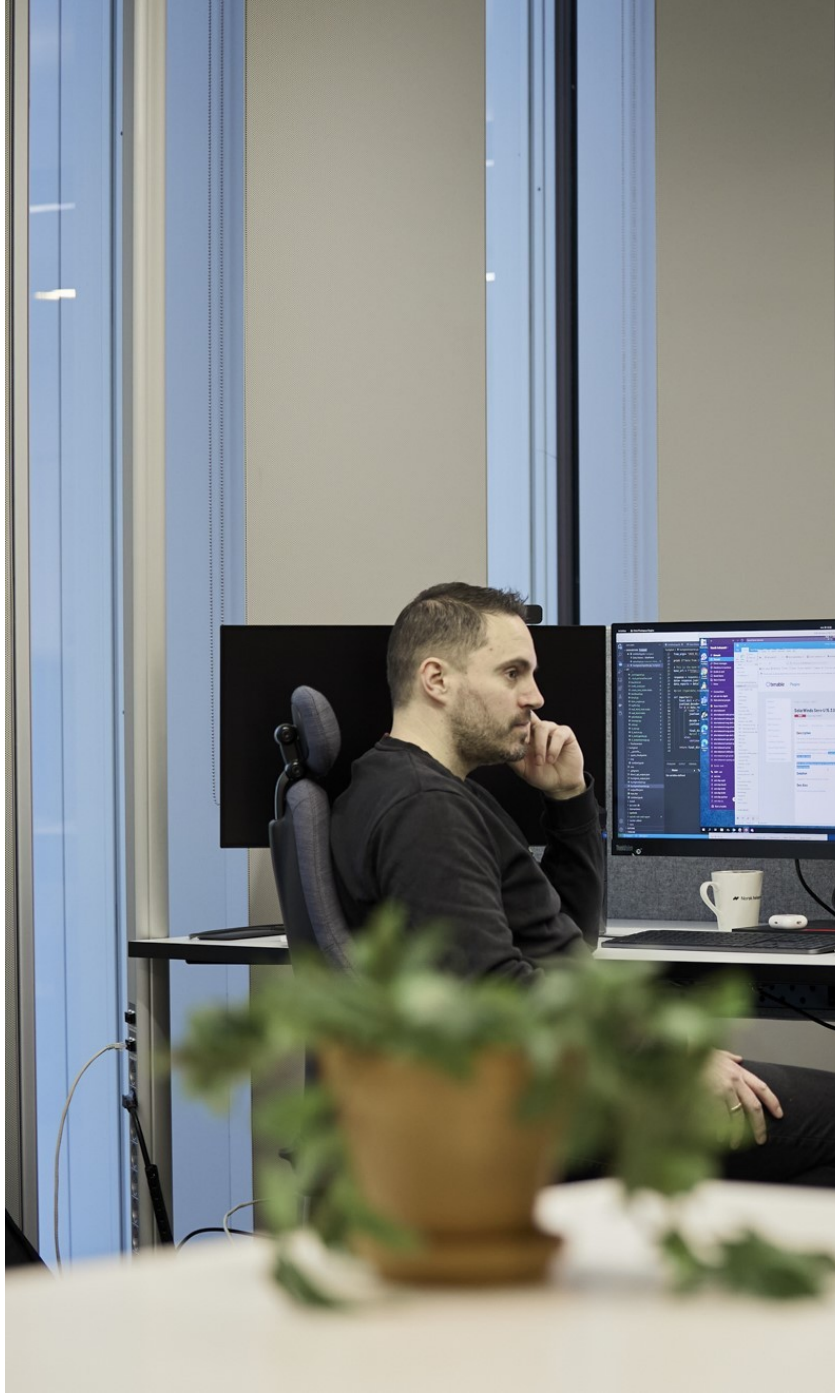
Vår kontaktinformasjon:
E-post: post@helsecert.no
Telefon: 24 20 00 00 – spør etter HelseCERT. Tilgjengelig 24/7 for akutte hendelser.

Webinarer

Vi har fortsatt med webinarer og har gjennomført ni planlagte webinarer og ett ad-hoc gjennomgang 2023.

Av de ni var fire webinar med tema logging, to situasjonsbilde m.m.,et om en hendelse og så avsluttet året med fokus på svakheter i flerfaktor og phishingresistent autentisering.

Vi planlegger å fortsette med jevnlige webinarer så lenge vi opplever at det er interesse og vi har aktuelle tema å snakke om.



Informasjondeling – NBP

Antall varsler sendt til NBP-saarbarhet i 2023

120

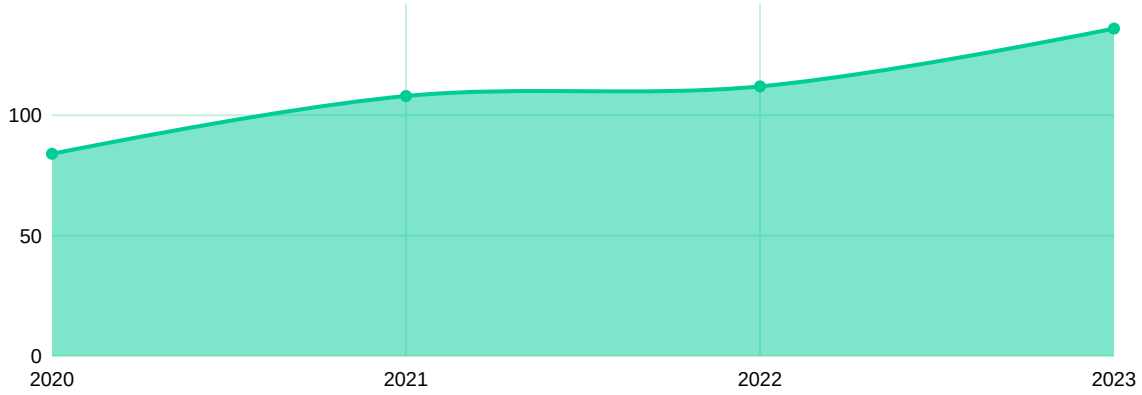
▲18

Antall varsler sendt til NBP-trussel i 2023

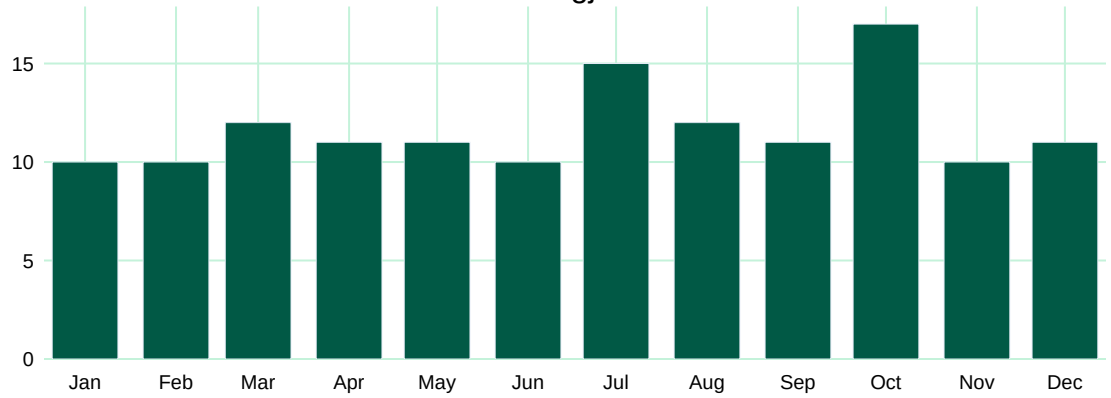
16

▲6

Trend antall varsler siste 4 år



Varsler sendt gjennom 2023



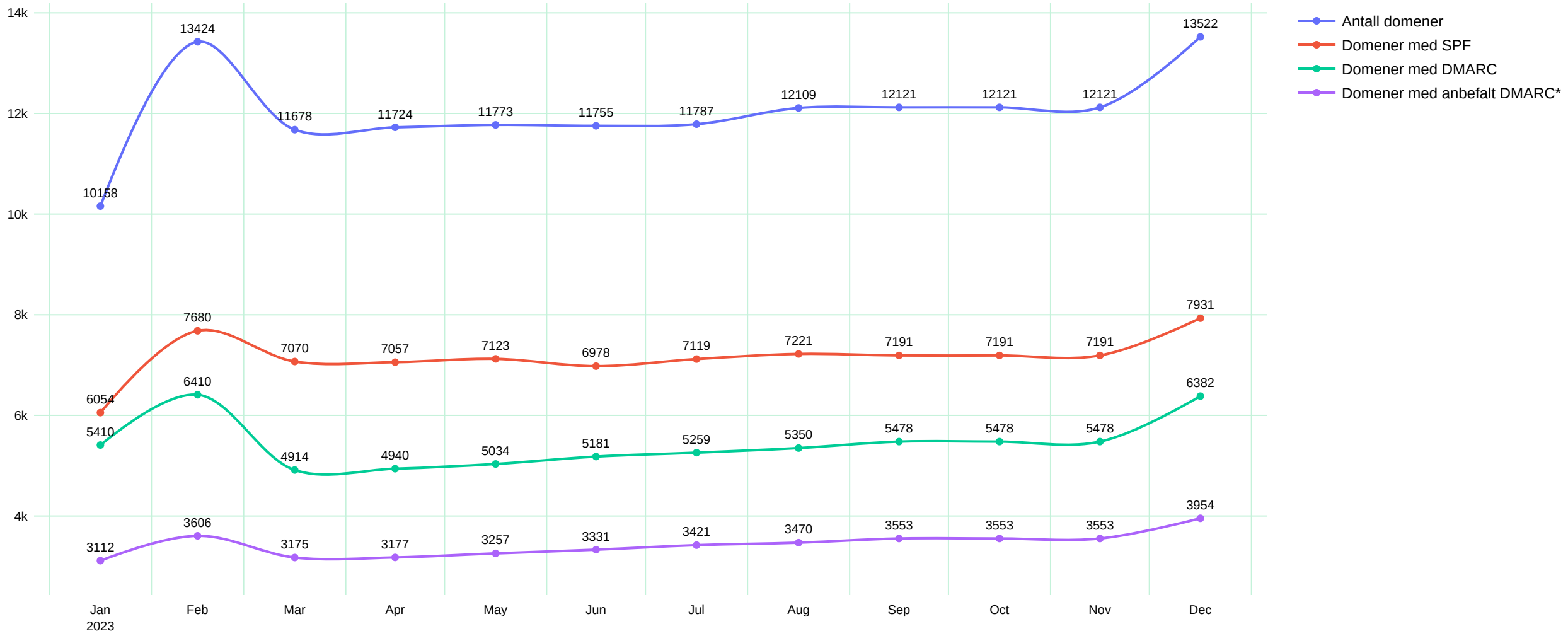
Tilbakeblikk 3. tertial 2023

Trend sårbarheter mot Internett – NBP

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

Vi ser dessverre ingen positiv utvikling i bruk av DMARC i løpet av 2023. Vi oppfordrer alle til å bruke egen oversikt for e-postsikkerhet i denne rapporten og følge vår guide for å implementere DMARC. Kontakt oss dersom dere har spørsmål: post@helsecert.no.



Tilbakeblikk 3. tertial 2023

Hendelser

Noen utvalgte hendelser vi har jobbet med i 3. tertial 2023.

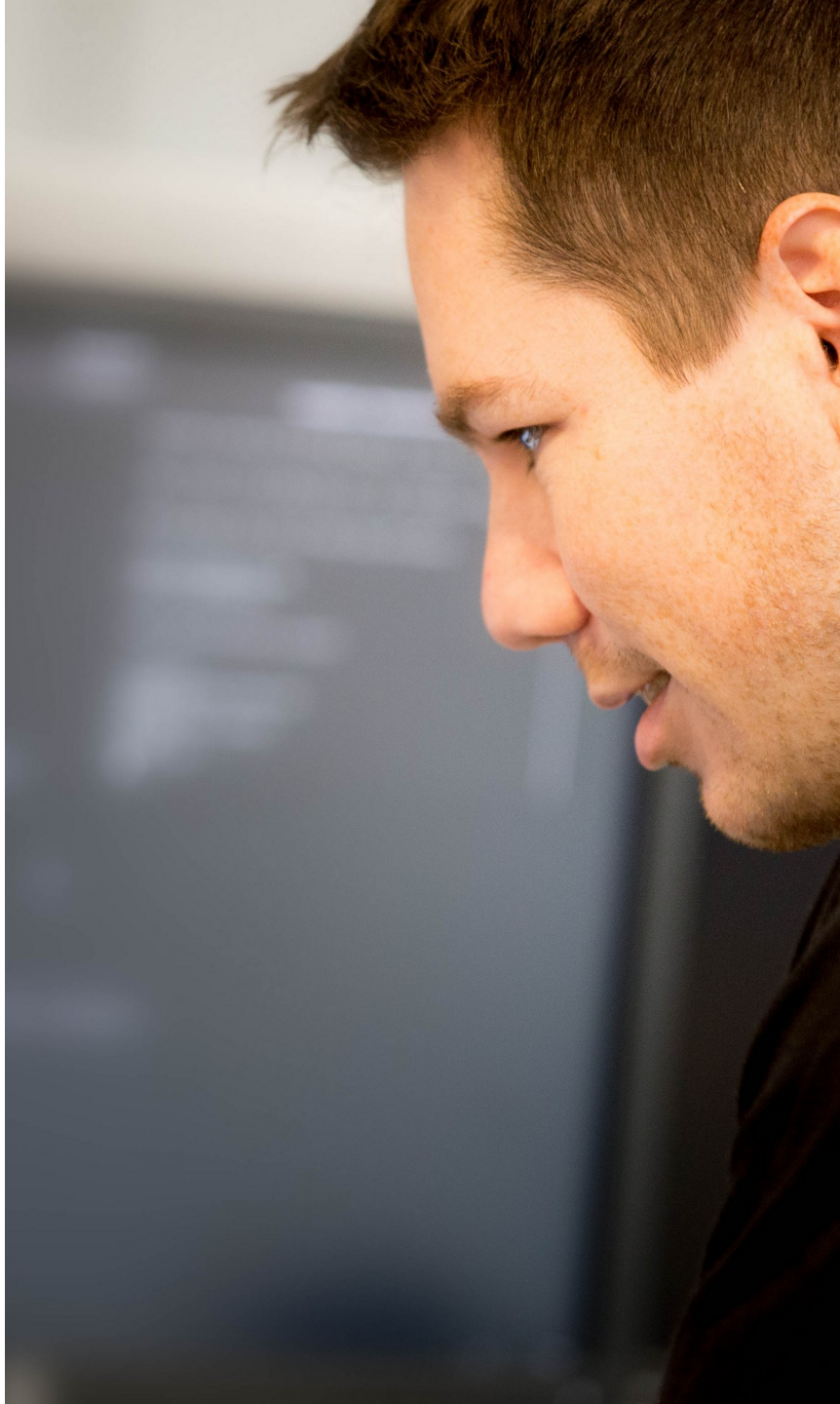
MFA-phishing – flere virksomheter kompromittert
I november og desember registrerte vi en markant økning i M365-phishing som bruker teknikker for å omgå multifaktorautentisering (MFA). Verktøy som benytter disse teknikkene er offentlig tilgjengelige, og de finnes i former som er supportert på ulike måter for å gjøre det enkelt for kriminelle. Rent teknisk er det sesjonscookies som hentes ut og brukes av angriper. Fordi disse ofte har begrenset varighet vil angriper normalt raskt logge inn på aktuell konto og starte sitt arbeid her.

Dette arbeidet består eksempelvis av sikring av tilgang på lengre sikt og kartlegging av både e-post og dokumenter på onedrive/sharepoint/teams, og vil i praksis være umulig for offeret å se eller oppdage. Hvis kartleggingen viser at offeret anses som "interessant", så vil kontoen benyttes til mer målrettet svindel/angrep, enten mot kolleger eller kunder som det er løpende dialog mot. Det er her vi ser høyest skadepotensiale. Her kan man eksempelvis se for seg at svindler ser eller tar over kommunikasjon knyttet til faktura/bankkonto/innkjøpsordrenummer, slik at virksomhetens systemer for å forhindre svindel ellers blir omgått.

Hvis offeret ikke anses som interessant, vil normalt kontoen benyttes for å sende ut nye phishing-e-poster til kontakter og andre man har utvekslet e-poster med, noe som øker sannsynligheten for påfølgende kompromitteringer. Vi er svært bekymret for denne utviklingen, og økningen i denne typen phishing og konsekvensen for virksomheten ved en slik kompromittering gjør at vi sterkt anbefaler å etablere phishingresistent autentisering, spesielt for M365. Start med administrator- brukere. Vi viser til vårt webinar om dette for ytterligere anbefalinger og tiltak.

Hackergruppe hevdet å ha stjålet data fra Stavanger kommune
En kjent hackergruppe annonserte i begynnelsen av oktober at de hadde stjålet data fra Stavanger kommune og truet med å publisere data. Vi bisto med rådgiving og koordinering med IRT og NCSC, samt analyse av logger. Det oppsto tidlig tvil om hvorvidt annonseringen fra hackergruppen var korrekt da det ikke ble funnet tegn på kompromittering hos kommunen.

Dette ble senere bekreftet når gruppen publiserte data og det viste seg at publiseringen ikke inneholdt informasjon fra Stavanger kommune. Analyse av innholdet bekrefter at dataen stammet fra virksomheter som ikke har kjente knytninger mot kommunen. Innholdet stammer fra et mindre eiendomsselskap og et verksted på Østlandet. Vi antar at data stammer fra et annet angrep mot et IT-selskap som leverer driftstjenester mot små og mellomstore bedrifter. Hendelsen fikk en del omtale i media, deriblant i NRK.



Hendelser

Coinminer på Citrix NetScaler
En angriper utnyttet en sårbarhet (CVE-2019-19781) til å plante en Coinminer. Coinminere installeres av kriminelle på kompromitterte systemer for å (mis)bruke virksomhetens datakraft til å generere krypto-valuta, og er ofte noe vi ser brukt i første angrepsbølge/masseutnyttelse når kode for utnyttelse av sårbarheter i internetteksponert infrastruktur blir offentlig tilgjengelig. Hvis sårbarheten ikke lukkes raskt nok vil man ofte også se ransomwareangrep noe senere. Hendelsen ble oppdaget ved en tilfeldighet når virksomheten ettergikk trafikk som matchet "botnet filter" i brannmurlogger.

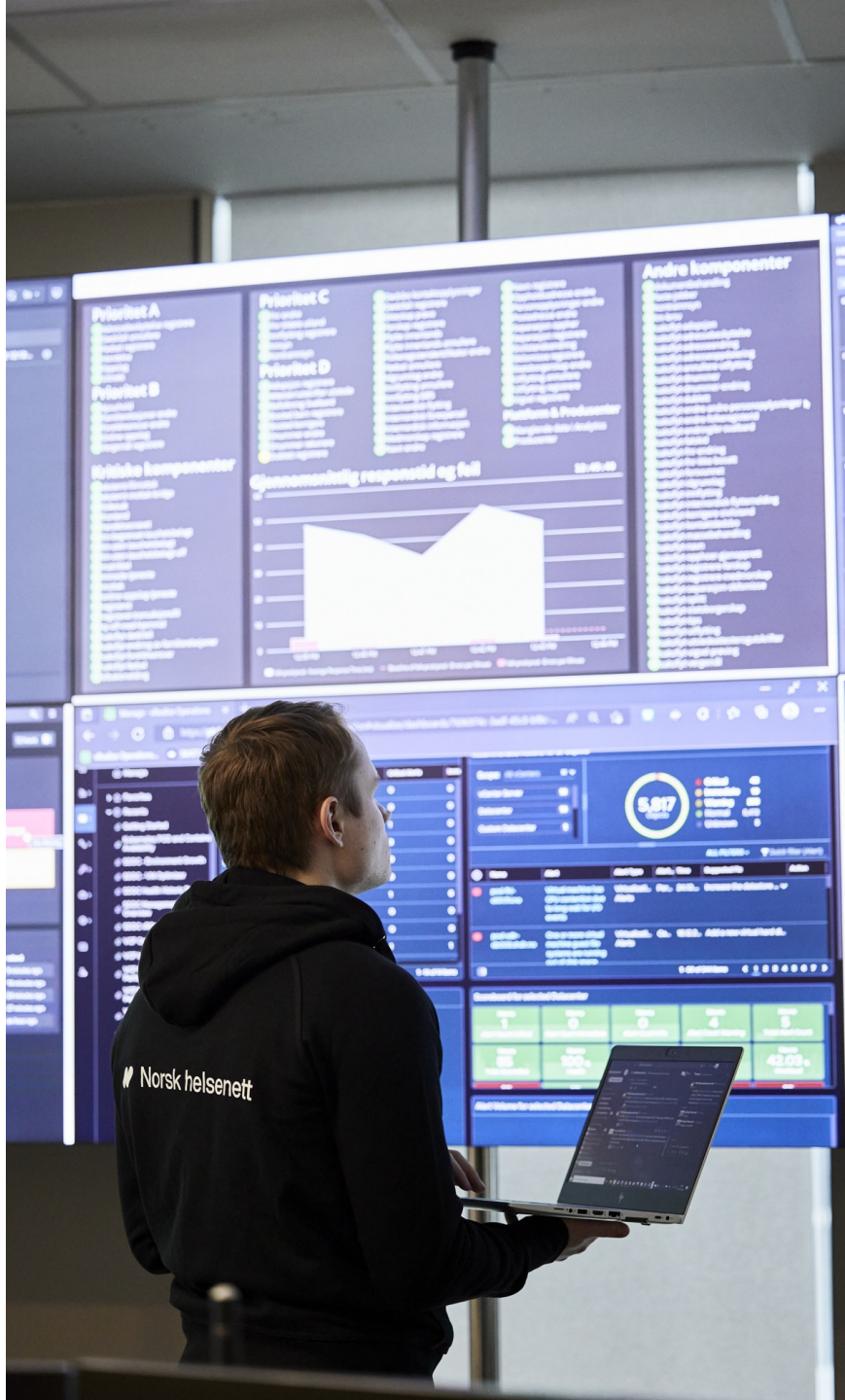
Analyse av image fra det kompromitterte systemet avdekket at Citrix NetScaler-enheten ble kompromittert så langt tilbake som 12. januar 2020. Det gikk da en svært bred kampanje som traff en rekke virksomheter, blant annet i vår sektor. Basert på historikk er vi kjent med at enheten ble oppdatert og sårbarheten lukket samme dag som den ble kompromittert, men uten at oppdateringen fjernet kompromitteringen.

Vår vurdering er at Citrix NetScaler-enheten var sårbar i et lite tidsvindu mens det foregikk meget bred utnyttelse sårbarheten, men at den ble oppdatert raskt nok til å unngå mer alvorlige kompromitteringer. Siden kompromitteringen skjedde langt tilbake i tid har det ikke vært mulig å identifisere mer relevant loggdata.

Coinmineren var satt opp til å kjøre som en cron-jobb. Basert på funnene her er det også rimelig å anta at kompromitteringen kun har medført Coinmining fram til neste gang NetScaler-enheten ble startet opp, siden selve Coinmineren ble slettet etter hver kjøring. Vi er også kjent med at infrastrukturen knyttet til Coinmineren ble tatt ned noen dager senere.

Vi har bistått med analyse av brannmurlogger samt image av den kompromitterte enheten.

Hendelsen skjedde hos en kommune. Vi er kjent med at det i januar 2020 var flere kompromitteringer av Citrix Netscaler-enheter, men de andre tilfellene vi kjenner til ble identifisert og ryddet opp i som et ledd i undersøkelsene som ble gjort. Siden dette må sjekkes lokalt på hver instans kan vi ikke garantere tilsvarende kompromitteringer hos flere virksomheter i helse- og kommunesektoren.



Sårbarheter

Kritisk sårbarhet i Citrix NetScaler – flere sårbare enheter i sektoren
En kritisk sårbarhet i Citrix NetScaler ADC/Gateway (CVE-2023-4966) ble i oktober aktivt utnyttet. Kode for å utnytte sårbarheten ble etterhvert publisert.

Varsel ble sendt til sektor samme dag som vi ble kjent med sårbarheten. En uke senere, da vi ble kjent med at sårbarheten var observert aktivt utnyttet, fikk vi prioritert skanning og identifikasjon av sårbare enhter og vi fulgte opp berørte virksomheter i sektoren. Vi fant da fire virksomheter som ikke hadde oppdatert sin instans. Vi er ikke kjent med kompromitteringer eller alvorlige konsekvenser som følge av sårbarheten i vår sektor, men vi er kjent med svært mange tilfeller av ransomware globalt hvor denne sårbarheten har vært veien inn.

Vi ønsker å fremheve at hurtig oppdatering av Citrix NetScaler ADC/Gateway ifm denne sårbarheten etter all sannsynlighet har forhindret flere alvorlige hendelser som ellers ville funnet sted i sektoren.

Kritisk sårbarhet i Cisco IOS XE-webgrensesnitt – tre virksomheter rammet
Mandag 16. oktober klokken 18:40 ble vi kjent med en kritisk nulldagssårbarhet i Cisco IOS XE-webgrensesnitt. Sårbarheten var på dette tidspunktet allerede aktivt utnyttet av en eller flere aktører for å legge inn en bakdør på Cisco IOS XE-enheter. Sårbarheten lar en uautentisert angriper lage en administratorbruker som har fullstendig kontroll over enheten.

Varsel ble sendt ut til sektoren 20:55 samme kveld. Vi iverksatte også umiddelbar skanning og kartlegging for å avdekke sårbare og kompromitterte enheter i sektoren.

Til sammen fem virksomheter med sårbare enheter ble avdekket og varslet. Hos tre av disse fikk vi bekreftet kompromittering som følge av utnyttelse av sårbarheten. Alle tre fikk raskt ryddet opp kompromitteringen og vi er per nå ikke kjent med alvorlige konsekvenser som følge av disse kompromitteringene. Alle virksomhetene er i kommunesektoren.

Erfaringer fra inntrengingstester - 2023

I løpet av året har vi utført inntrengingstester i spesialisthelsetjenesten, kommuner, etater og av ulike systemer. Hos virksomheter som har blitt testet over flere år av oss ser vi at trenden er god. Vi finner færre svakheter, og svakheter vi har funnet tidligere år har blitt utbedret. Hos de virksomhetene som er mest modne finner vi nå få eller ingen svakheter i Active Directory og vi gjør derfor mer testing av andre interne systemer, terminalservere og medisinskteknisk utstyr.
I tillegg til våre inntrengingstester har vi mottatt Hurtigtest-rapporter fra en god del NBP-medlemmer som gir oss god innsikt i status for sektoren. Hurtigtest har nylig fått utvidet funksjonalitet med sjekk for typiske sårbarheter i sertifikathåndtering (AD CS) og sensitive data på delte filområder. Resultater fra disse sjekkene vil vises bedre fra 2024. Samlet gir disse aktivitetene oss et bilde av sektoren som oppsummeres i punktene under.

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. Mangel på lister med forbudte passord gjør at de de mest sannsynlige passordene innenfor policy blir brukt. Kontoer med svake passord utgjør en høy risiko.

Anbefaling: Følg vår passordpolicy på helsecert.no. Benytt Hurtigtest for å avdekke svakheter. Se vårt webinar om intern passordknekking.

Ta i bruk verktøy som kontrollerer passordkvalitet, for eksempel har Powershell-modulen DSInternals en funksjon som heter Test-PasswordQuality. Den finner blant annet gjenbrukte passord.

2

Interne systemer som ikke følger beste praksis
Vi ser at internt utviklede systemer ofte har mindre fokus på sikkerhet. Dette gir 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 passord og annen sensitiv informasjon i filer på delte filområder. Konfigurasjonsfiler, administrasjonsskript og backupfiler er gjengangere. Vi har også begynt se etter personnumre i filer på delte filområder, og her finnes det en del som tidligere er uoppdaget.

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

4

Feilkonfigurert tilgangsstyring for sertifikater (AD CS)
Mangelfull tilgangsstyring av hvem som kan utstede sertifikater i Active Directory kan utnyttes til å eskalere rettigheter. Generelt er det mangelfull tilgangsstyring av hvem som kan utstede et maskinsertifikat eller mangelfull integritetssjekk av hvem som ber om et sertifikat.

Anbefaling: Blokker muligheten for utstedelse av sertifikater på vegne av vilkårlige brukere. Benytt Hurtigtest for å avdekke svakheter.

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 gjør endepunktsikring på terminalservere minst like god som på klientmaskiner.

6

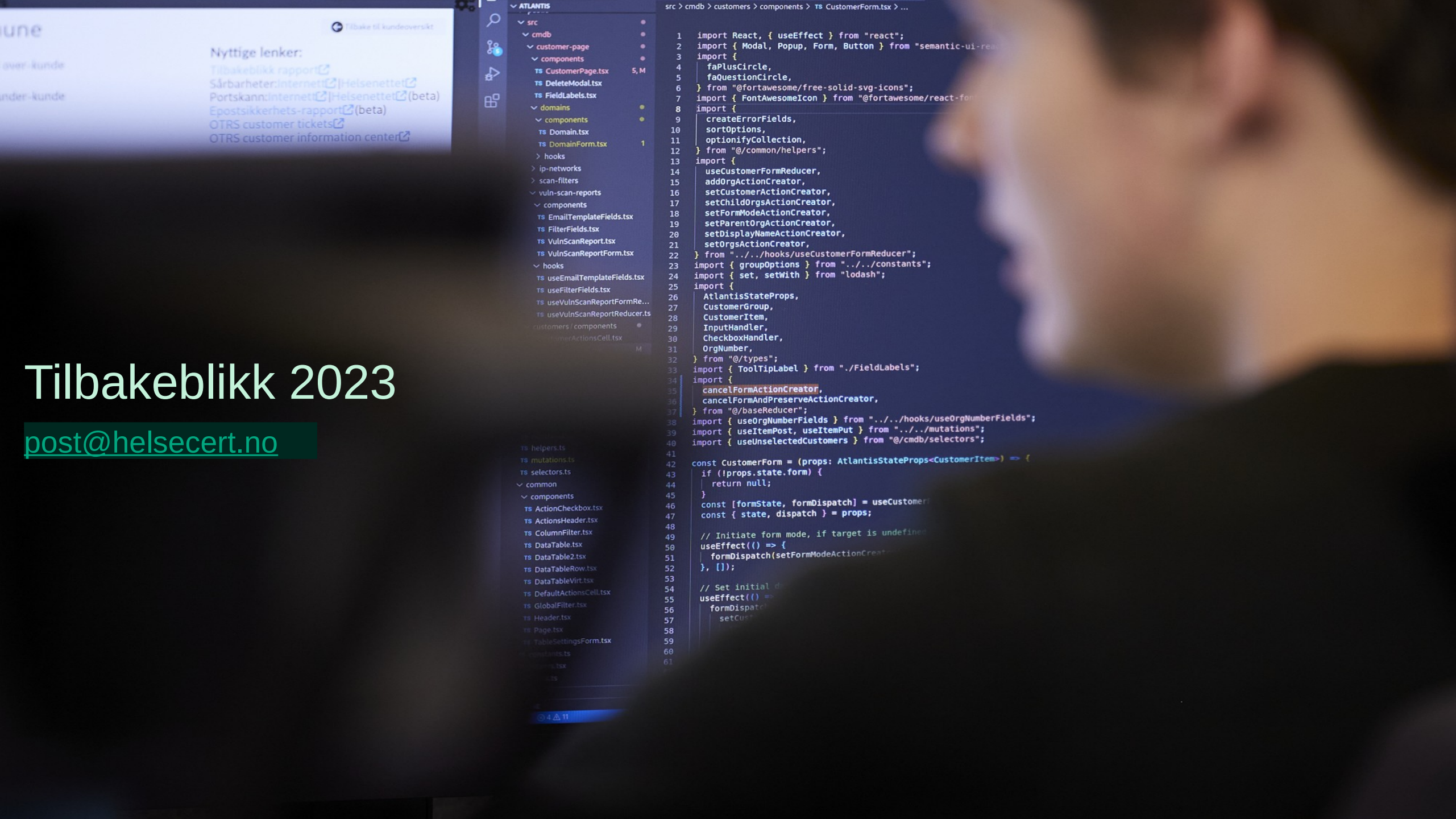
Dårlig sikring av interne systemer
Telefoner, printere, byggteknisk og medisinskteknisk utstyr har oftere manglende tilgangsstyring eller fabrikkpassord som er lett å finne for en angriper. Dette åpner for muligheten for å forstyrre driften av virksomheten og gir angriper muligheten til å etablere fotfeste. Det finnes også en del programvare og fastvare som ikke er oppdatert, og derfor har kjente sårbarheter. For AD-innmeldte maskiner er ofte operativsystemet oppdatert, mens annen programvare kan lide av manglende vedlikeholdsarbeid. For systemer utenfor AD finnes det i tillegg mye manglende oppdateringer til operativsystemer.

Anbefaling: Skift fabrikkpassord på nytt utstyr før det kobles til nettverk. Sett sterke administratorpassord. Slikt utstyr bør stå i egne nettverkssoner med administrasjonsgrensesnittene tilgjengelig kun fra dedikerte maskiner

Trusselvurdering

Oppdatert versjon av vårt situasjonsbilde er publisert på våre nettsider.

- Det er meget sannsynlig at fremmede stater ser på helsesektoren som et mål for spionasje.
- Vi mener det er sannsynlig at norsk helse- og kommunesektor vil treffes av angrep fra aktører som et ledd i det generelle arbeidet til statlige eller stats-sponsede etterretningstjenester.
- Vi mener det er meget sannsynlig at norsk helse- og kommunesektor vil treffes av angrep fra organiserte kriminelle grupper.
- Vi mener det er meget sannsynlig at norsk helse- og kommunesektor vil treffes av angrep fra hacktivister. Typisk tjenestenektangrep.



Tilbakeblikk 2023

post@helsecert.no