Norsk helsenett

HelseCERTs Tilbakeblikk

Nøkkeltall og oppdateringer for 2022

Innhold

Forord

Hei og godt nyttår til alle medlemmer i Nasjonalt beskyttelsesprogram. Denne versjonen av HelseCERT tilbakeblikk inneholder vår oppsummering av 3. tertial samt data og statistikk for hele 2022.

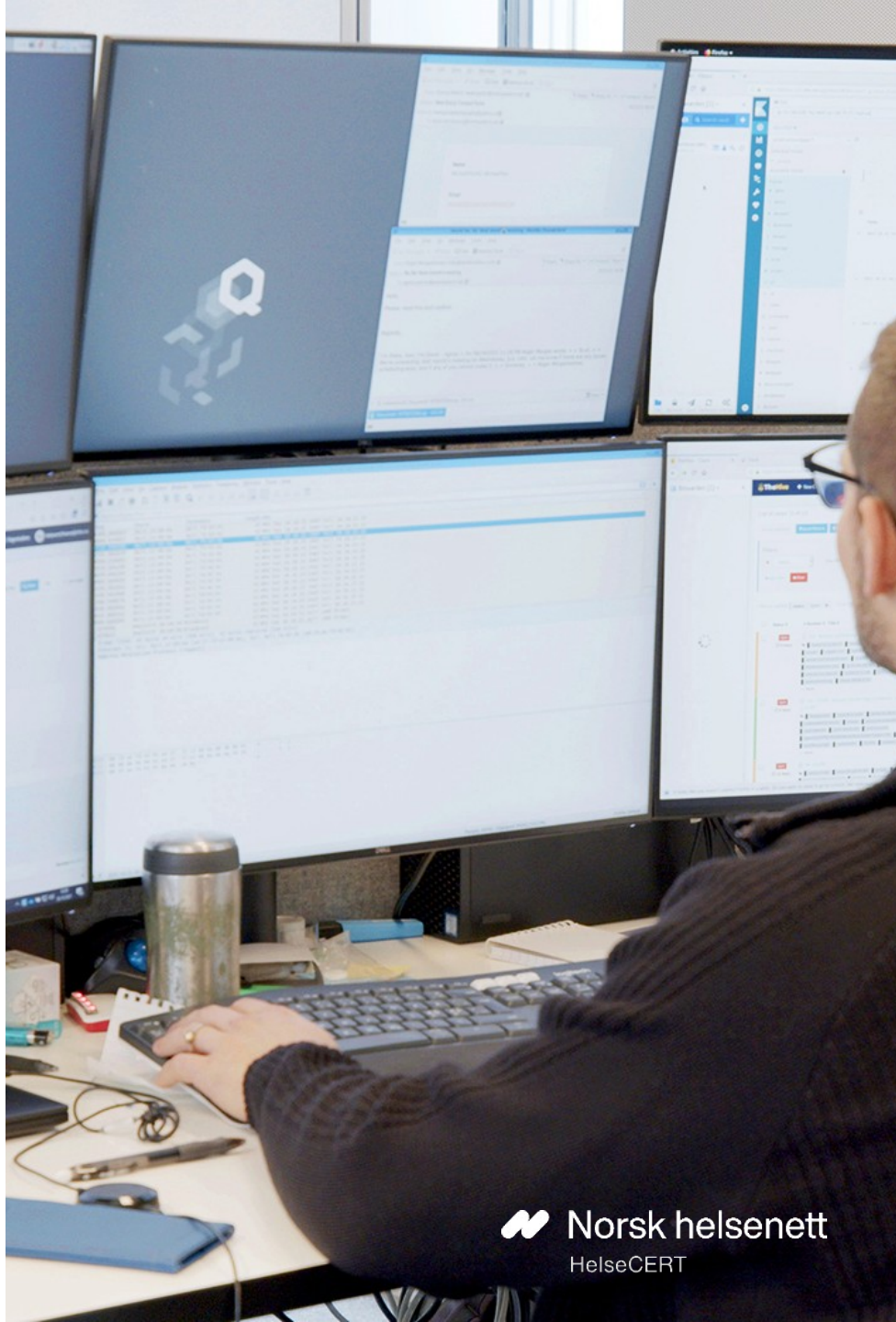
Formålet er å dele nyheter fra oss i HelseCERT samt gi dere innsikt i statistikk og trender for sektoren. 2022 har vært preget av krigen i Ukraina og endringen den har medført for den sikkerhetspolitiske situasjonen i Europa. PST har meldt om økt etterretningstrussel mot Norge, det er meldt om utstrakt droneaktivitet rundt kritisk infrastruktur og sabotasje mot gassrør i Østersjøen. Beredskapen i Norge har blitt skjerpet og en rekke tiltak har blitt innført for å motstå ulike former for trusler mot Norge.

For å sikre oss enda bedre mot dataangrep og øke helsesektorens robusthet trenger vi at alle bidrar. Vi må bli enda mer bevisste på hvilke trusler som kan ramme oss og hvordan vi kan beskytte oss. Det er viktig at alle i sektoren bidrar med å beskytte sin infrastruktur og sine systemer så godt som mulig. I sum vil det gjøre oss, helsesektoren og Norge, bedre rustet til å motstå sammensatte trusler.

Vi ønsker at dere bruker denne oppsummeringen fra oss til å få oversikt over trusler, anbefalinger og ikke minst hvilke tiltak vi anbefaler for akkurat din virksomhet.

Sammen gjør vi helsesektoren sikrere!

Med hilsen
HelseCERT



Situasjonsvurdering

Vurderinger

- Det er meget sannsynlig at fremmede stater ser på helsesektoren som et mål for spionasje.
- Det er meget sannsynlig at virksomheter i helsesektoren blir utsatt for økonomisk motiverte angrep.
- Det er sannsynlig at virksomheter i norsk helsesektor blir truffet av angrep gjennom en verdikjede.
- Det er mulig at skadevarekampanjer påvirker pasientbehandling.
- Det er mulig angrep fra hacktivister vil ramme nettsider og tjenester i sektoren

Oppdatert versjon av HelseCERTs situasjonsbilde er publisert på våre nettsider:

https://www.nhn.no/om-oss/Personvern-og-informasjonssikkerhet/helsecert/publikasjoner/situasjonsbilde-2022

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.

Se også NSMs fem effektive tiltak mot dataangrep.

Situasjonsbildet

Verdikjedeangrep har vokst til å være en av truslene som krever fokus i tiden fremover. En bedrifts verdikjede er ofte uoversiktlig, komplisert og flytende. Et verdikjedeangrep utnytter den økte angrepsflaten bruken av programvare, kode og tilganger fra eksterne medfører. Det siste året har vi sett eksempler på verdikjedeangrep gjennom alt fra utnyttelse av sårbarheter hos store veletablerte leverandører til sårbarheter i små kodebibliotek

Utpressingsaktører. Det siste året har vi sett mange – og store – destruktive angrep fra utpressingsgrupper. Den generelle fremgangsmåten er lik som i de siste årene - etter kompromittering jobber trusselaktøren for å få kontroll over så mange av bedriftens systemer som mulig, før sensitive data eksfiltreres og systemene krypteres.
Etter kryptering er det gjerne tre forskjellige metoder som brukes for å tjene penger på angrepet:

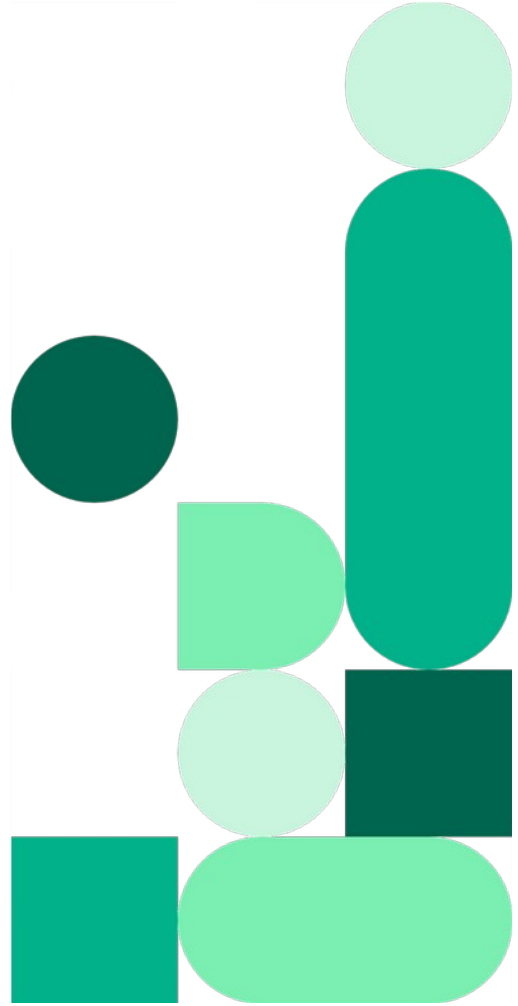
- Kreve betalt for dekryptering
- Kreve betalt for at data ikke publiseres
- Presse penger fra personer rammet av datalekkasjen

Svindlere. Tall fra internasjonale organisasjoner viser at svindel medfører store økonomiske tap for bedrifter. Profesjonelle svindelgrupper kjører operasjoner der de gjør grundig forarbeid og lærer seg å kjenne offeret sitt. I likhet med utpressingsgruppene varierer metodene og målene. Svindlene vi ser kan grovt grupperes slik:

- Fakturasvindel - hvor svindlerne forsøker å skaffe legitime fakturaer og endrer kontonummer på disse.
- Direktørsvindel - hvor de forfalsker kommunikasjon så den ser ut til å komme fra en direktør som trenger en "konfidensiell hastebetaling".
- Business Email Compromise - hvor svindler skaffer tilgang til e-postkommunikasjon for å skreddersy svindler basert på innsideinformasjon.

Spionasje. Forskningsdata er et verdifullt mål for trusselaktører. Sykehus og andre helseinstitusjoner som bidrar til, og har tilgang til forskningsdata, må være forberedt på at trusselaktører aktivt forsøker å skaffe tilgang til disse. Dette har spesielt vært dagsaktuelt under C COVID-19-pandemien og vil fortsette å være aktuelt framover.

Sabotasje. Ukrainas strømforsyning ble i 2015 utsatt for en serie destruktive angrep som resulterte i blackout over store deler av landet. Angrepene er blitt attribuert til russiske statlige grupper. Angrepene var satt opp til å ramme størst mulig del av landet samtidig. Russland forsøkte å gjenta samme typen angrep i april 2022, men denne gangen ble angrepet avverget. Vi registrerer at cyber er brukt til sabotasje av kritisk infrastruktur. Dette er så langt ikke observert innen helse, men må vurderes som et mulig mål.



Nytt fra HelseCERT

Hurtigtest

HelseCERT Hurtigtest er en automatisert sikkerhetstest som tar for seg de mest grunnleggende svakhetene våre pentestere normalt finner ute i sektoren. 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. Over hundre virksomheter har lastet ned Hurtigtest og mange svakheter er blitt utbedret.

Vi oppfordrer alle medlemmer til å kjøre Hurtigtest.

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. I første 1. tertial 2023 vil vi sette et ekstra fokus på logging og setter opp en serie med webinarer hvor dette er tema.

I tilknytting til webinarene vil vi også publisere våre logganbefalinger på helsecert.no.

Sikkerhetsskanning

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

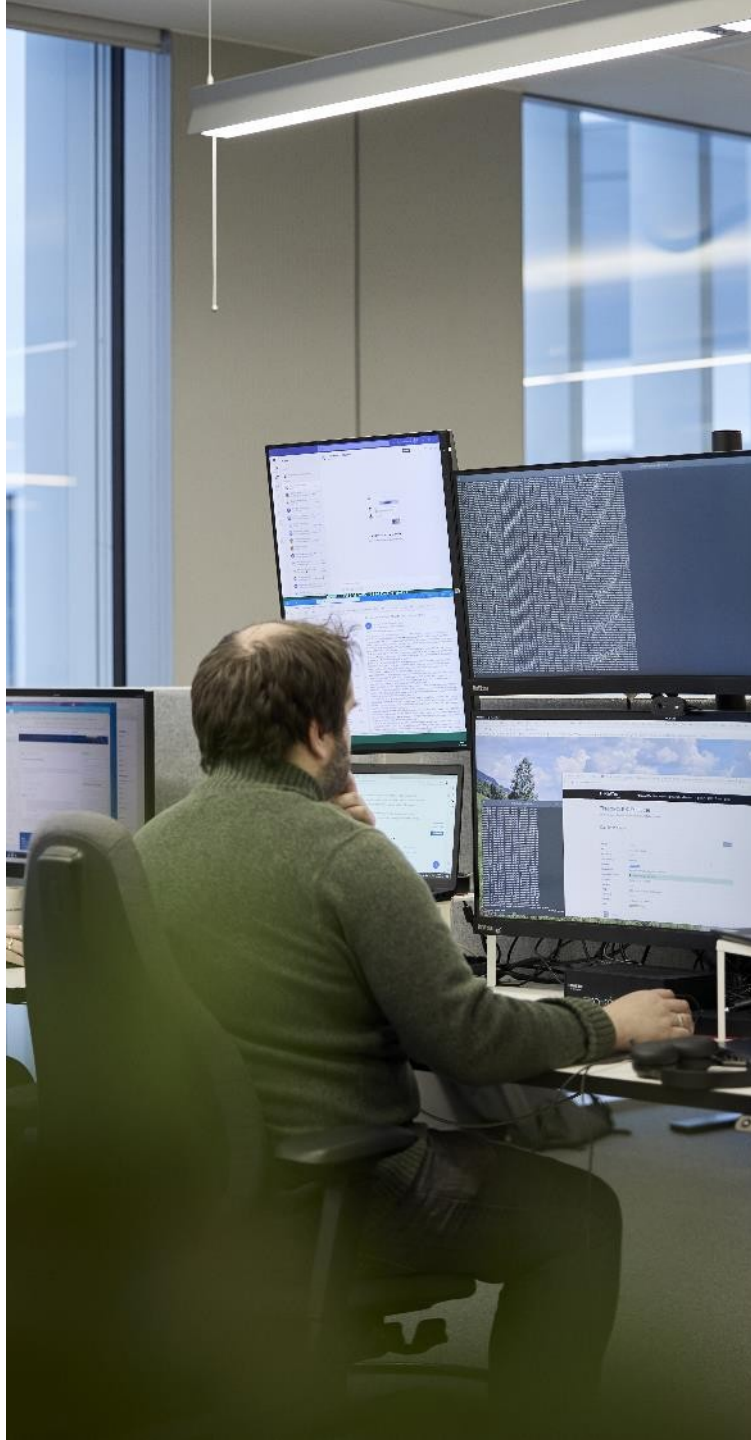
Vi jobber løpende med videreutvikling og oppdatering av vår sikkerhetsskanning. Vi har i løpet av siste tertial tatt i bruk flere kilder i datainnsamlingen og vi vil i dette tertialet inkludere disse i vår automatiserte varsling ut til dere. Dette for å øke kvalitet og innhold på varslene.

I forbindelse med aktivt utnyttelse av en sårbarhet i Exchange server / Outlook Web Access sendte vi i desember ut varsel til 29 virksomheter som etter våre kartlegginger hadde servere sårbare for utnyttelse. Mange av disse fikk med bakgrunn i varslet raskt patchet eller tatt server av nett. De vi ikke fikk svar på ble ringt opp dagen etter.

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

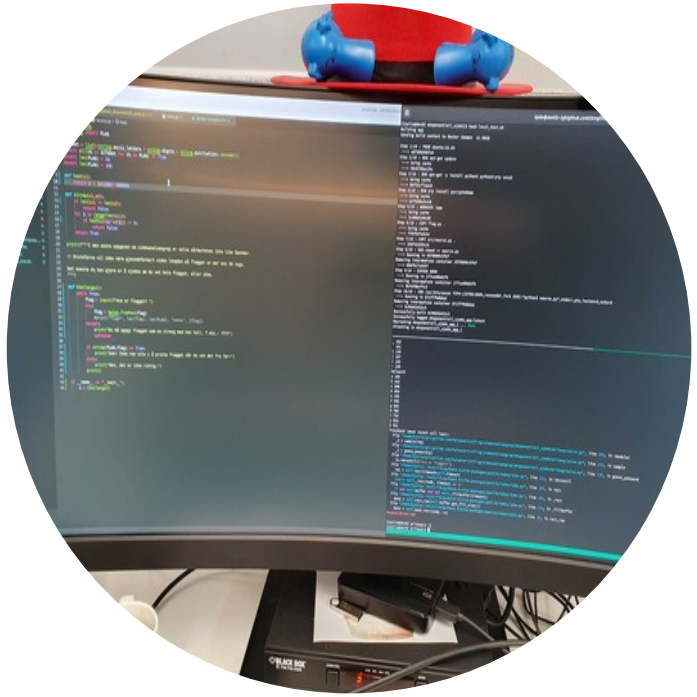


Resultater inntrengingstester

Vi har i 2022 gjennomført inntrengingstester i helseregioner, kommuner, etater og andre virksomheter i sektoren. Vi ser en positiv trend i sektoren ved at vi finner færre svakheter og at svakheter vi har funnet tidligere år har blitt utbedret. Dette gjelder særlig for de større virksomhetene. Generelt opplever vi dessverre lavere modenhet hos mindre virksomheter.

Testingen omfatter tjenester eksponert på internett samt interne tjenester som Active Directory(AD), terminalservere, byggtekniske-/SD-anlegg, medisinsk utstyr m.m.

I tillegg til funn fra gjennomførte inntrengingstester har vi også fått tilbake et stort antall Hurtigtest rapporter. Samlet gir dette oss et godt bilde av status i sektoren. På neste side oppsummerer vi de mest sentrale og vanligste funnene vi avdekker og som vi anbefaler at dere følger opp i egen virksomhet.



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 også interne utviklingsprosesser følger beste praksis. Fas ut gammel 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 adminpassord. 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.

Hendelser siste periode

Raspberry Robin – skadevare via minnepinner.

I den siste tiden så har vi fått rapporter fra en god del virksomheter som har fått skadevaren Raspberry Robin via bruk av minnepinner. Denne skadevaren bruker angrepsteknikker som omgår mange av de tradisjonelle sikringstiltakene. Den spres ved at bruker lures til å kjøre/åpne en snarvei fra en infisert minnepinne. Minnepinnen har mest sannsynlig igjen blitt infisert fra andre infiserte maskiner. Raspberry Robin ser ut til å primært bli brukt til å skaffe et første fotfeste inn i en virksomhet.
Hvis noen har hatt infeksjoner med Raspberry Robin ønsker vi gjerne at dere tar kontakt med oss. Vi har laget en teknisk analyse av Raspberry Robin som er tilgjengelig på github.

Angrep med bruk av USB-rubber-ducky

Vi har jobbet med en hendelse hvor inngangsvektor var at angriper fysisk satte en USB-enhet inn i maskin hos rammet virksomhet. Angrepet ble gjennomført med bruk av hackingverktøyet USB Rubber Ducky. Dette er en USB-enhet som kan fortelle PC-en den plugges inn i at den er et tastatur. En angriper kan programmere enheten til å sende kommandoer til maskinen den plugges inn i og dermed kjøre store mengder forhåndsdefinerte kommandoer i løpet av kort tid.

Angriper forsøkte å opprette tilkoblinger ut mot ulike ressurser på internett, antakeligvis for å beholde tilgang til den aktuelle PC-en og å senere kunne bruke dette til videre angrep/bevegelse i nettverket. Den aktuelle PC-en var automatisk innlogget med fellesbruker, og angriper fikk tilgang til maskinen i kraft av å være pasient.

Følgende faktorer gjorde at angrepet mislyktes:

- grunnsikringen i form av standard sikkerhetsløsninger/anti-virus varslet virksomheten
- god effektiv håndtering av disse varslene gjorde at aktuell PC raskt ble tatt inn til analyse
- utvidet logging gjorde det mulig å identifisere hva som var forsøkt
- utgående brannmur/proxy-regler gjorde at internettilgang fra aktuell PC var begrenset, noe som senket tempo til angriper

Det er ingen tegn til at denne hendelsen var del av en større organisert kampanje. Hendelsen er politianmeldt.

Hendelser siste periode - fakturasvindel

Fakturasvindel
De siste årene har vi sett en profesjonalisering av økonomiske svindelgrupper. Fakturasvindel - hvor svindlerne forsøker å skaffe tilgang til legitime fakturaer og endrer kontonummer på disse, har vært noe vi har varslet om jevnt gjennom de siste årene. Det er viktig å vite at dette er profesjonelle svindlere, som har dette som fulltidsjobb og som bruker hele arbeidsdager på å lure en bedrift til å betale ut store pengesummer.

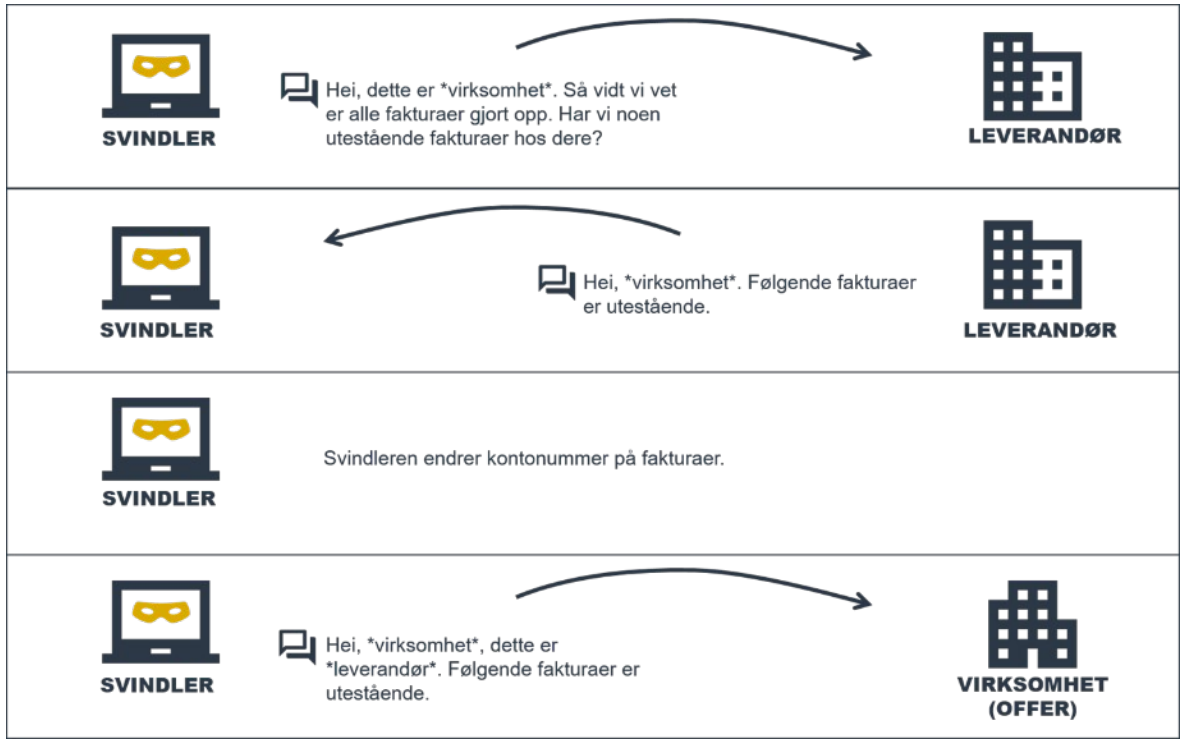
De jobber i team, har forskjellige spesialiteter – noen er f.eks. flinke til å sende falske eposter mens andre er gode på å lure et offer over telefon. Disse gruppene gjør gjerne grundig forarbeid, inkludert rekognosering, for å fremstå mest mulig troverdig ovenfor ofrene. De er villige til å kjøre operasjoner hvor de holder e-postdialoger gående over lang tid.

De kartlegger kunde/leverandørforhold, gjerne ved bruk av Doffin og / eller TED (Tenders Electronic Daily, EUs anbudsdatabase). Vi har sett avanserte svindelforsøk mot helsesektoren som har benyttet seg av dette, heldigvis uten hell. Vi vet at samme metode har vært vellykket mot andre bedrifter i Norge.

Svindlerne er dyktige på sosial manipulasjon, det vil si å lure mennesker til å gjøre det svindlerne vil at man skal gjøre. Dette gjør de ved å forfalske e-poster, utgir seg for å være leder i din bedrift, spiller på et tidspress (f.eks. «Denne regningen skulle vært betalt for flere uker siden, nå holder vi på å miste en viktig kontrakt / tjeneste.» «Jeg trenger at du gjør dette med en gang, det er viktig for meg.» De spiller også på tillitt, f.eks. ved å spørre en medarbeider om de «kan stoles på.»

På illustrasjonen kan dere se en vanlig måte de operer på. Aktøren utgir seg for å være «offeret» og kontakter en leverandør. Trusselaktøren spør leverandøren om vi (offeret) har noen utestående fakturaer. Leverandøren vil gjerne ha betalt og svarer med å sende over utestående fakturaer på e-post. Svindlerne endrer så betalingsinformasjon på fakturaen, går over til å utgi seg for å være leverandøren og sender over fakturene over til offeret og ber om at de betaler de utestående fakturane

Noen profilerte mediesaker har vært UiT – Norges arktiske universitet som ble svindlet for 12 millioner og Norfund som ble svindlet for hele 100 millioner. Vi er kjent med at det har vært nye vellykkede svindelforsøk i andre sektorer i løpet av siste tertial.



Norsk helsenett
HelseCERT

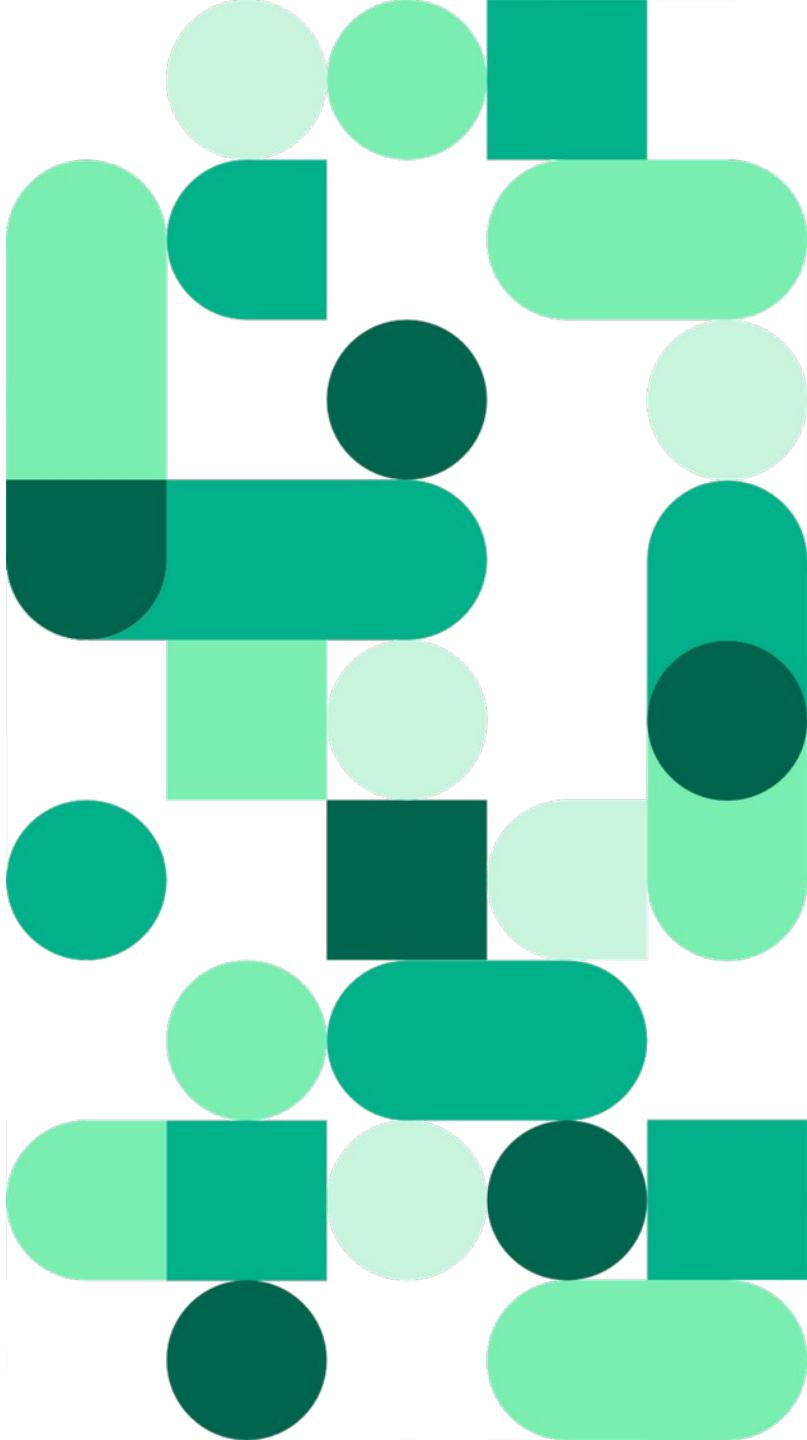
HelseCERT webinarer

Kommende webinarer:

Tema	Dato
HelseCERT tilbakeblikk 2022	13.01.2022
Sentral logging	10.02.2022
Logging Windows	10.03.2023
Logging Linux	14.04.2023
Logging brannmur/applikasjon	12.05.2023

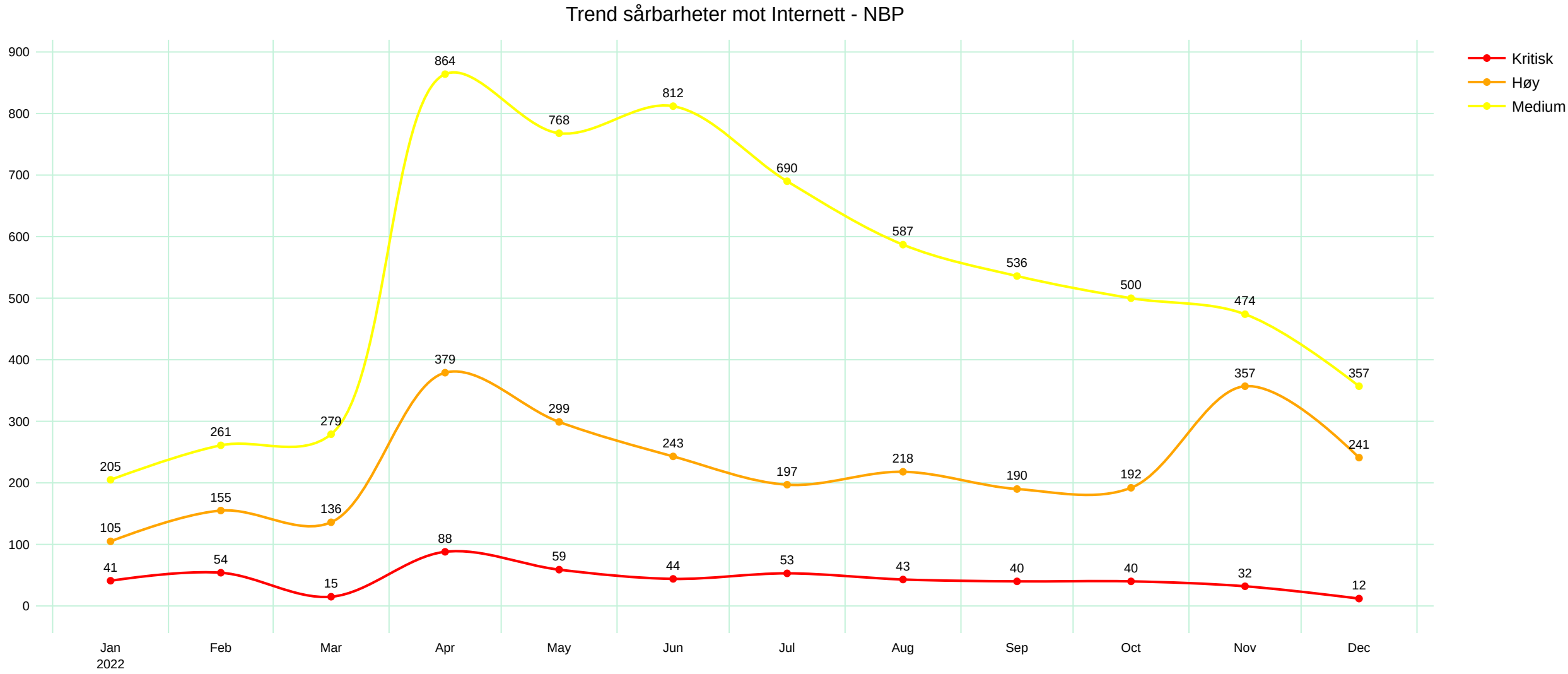
Tidligere webinarer:

Opptak av tidligere HelseCERT webinar er tilgjengelig på vår nettside:
https://www.nhn.no/om-oss/Personvern-og-informasjonssikkerhet/helsecert/webinarer



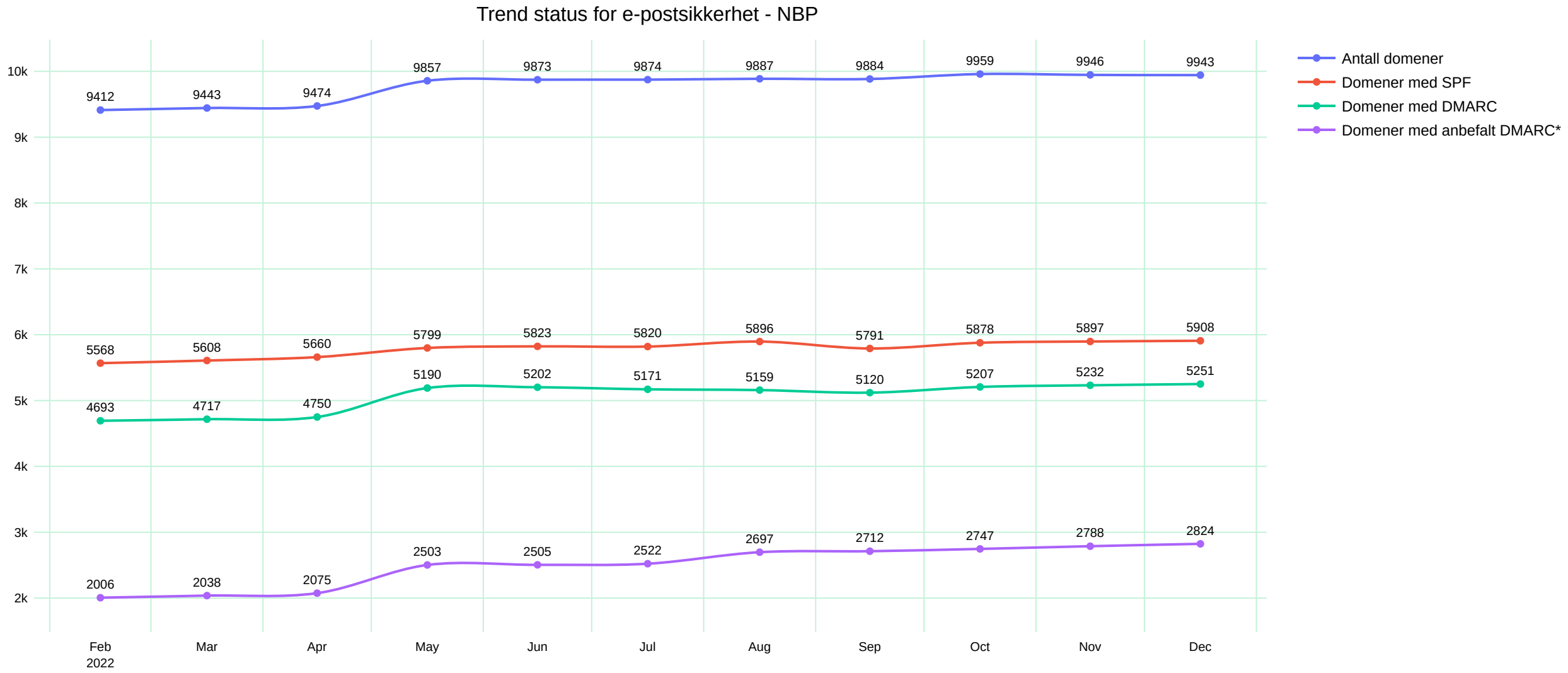
Statistikk for alle NBP medlemmer

Norsk helsenett
HelseCERT



Statistikk for alle NBP medlemmer

Norsk helsenett
HelseCERT



Kommentarer til statistikk for alle NBP medlemmer

Trend sårbarheter mot Internett – NBP

- Økningen i april skyldes hovedsakelig endringer vi har gjort ved at flere domener ble inkludert i skanningen.
- Økningen av sårbarheter i kategorien HØY i november er knyttet til end of life på en mye brukt PHP versjon.
- Overordnet ser vi en positiv trend med at sårbarheter lukkes og at grafen trender i positiv retning når vi tar høyde for at flere systemer blir skannet.
- Økningene gjennom året skyldes hovedsakelig forbedringer i vår skanning og økning i antall IP'er og domener som blir skannet. Når vi oppdager og varsler om nye ting ser vi at antall sårbarheter går raskt nedover etter varsel fra oss.
- Antall systemer (IP'er og domener) som blir skannet endres når nye virksomheter blir medlemmer og når eksisterende medlemmer gjør endringer.
- Antall systemer som blir skannet framkommer ikke av denne statistikken.

Trend sårbarheter for e-postsikkerhet – NBP

- Vi ser en svak positiv utvikling i antall domener med anbefalt DMARC policy med en total økning på 818 domener med anbefalt policy. Vi ser at en god del av denne økningen skyldes at nye domener som allerede hadde DMARC policy på plass har blitt inkludert i vår skanning.
- Vi oppfordrer alle til å bruke egen oversikt som følger lengre ned i denne rapporten og vår anbefaling på https://www.nhn.no/om-oss/Personvern-og-informasjonssikkerhet/helsecert/anbefalte-sikkerhetstiltak/e-postsikring/dmarc til å implementere DMARC.

NBP - Tjenester

- Anbefalte sikkerhetstiltak
- Blokkeringslister
- Brukernavn og passord på avveie
- Hendelseshåndtering
- Informasjonsdeling og forebygging
- Sikkerhetsskanning
- Situasjonsbilde
- Tilbakeblikk
- Webinarer
- Hurtigtest

For mer informasjon: helsecert.no

Ta kontakt på post@helsecert.no om du har spørsmål om noen av tjenestene.

Norsk helsenett
HelseCERT

HelseCERTs tilbakeblikk

Spørsmål og kommentarer kan sendes til post@helsecert.no

www.helsecert.no