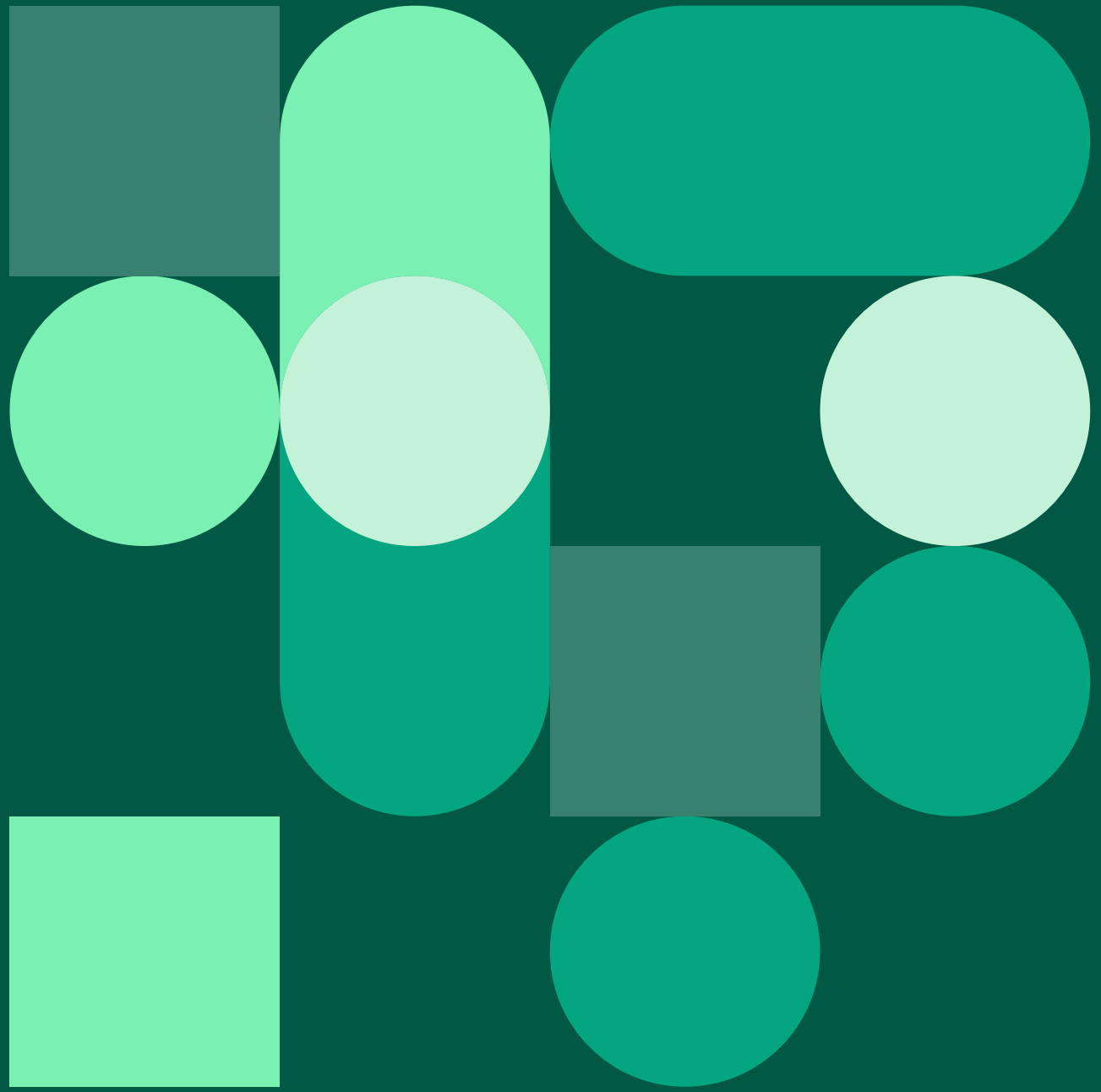
Norsk helsenett

HelseCERTs tilbakeblikk

Nøkkeltall og oppdateringer
1. tertial 2022



HelseCERTs tilbakeblikk 1.tertial 2022 – Nasjonalt beskyttelsesprogram (NBP)

Norsk helsenett
HelseCERT

HelseCERTs situasjonsbilde - Ukraina

Situasjonsbilde

- Vi kjenner per nå ikke til cyberhendelser i norsk helsesektor eller Norge for øvrig som kan knyttes direkte til situasjonen i Ukraina.
- Vi vurderer at risikoen mot helsesektoren er forhøyet. Dette gitt muligheten for at cyberangrep mot ukrainske mål direkte eller indirekte kan ramme tredjeparter
- PST melder om en økt etterretningstrussel mot Norge.
- Pro-russiske grupper gjennomfører tjenestenektangrep mot virksomheter i flere NATO-land. Virksomheter i Tsjekkia, Romania og Tyskland har nylig blitt rammet av slike angrep. Angrepene fører til nedetid på sidene som blir berørt, men utover nedetid så har disse angrepene små direkte konsekvenser.
- Vi må forvente at slike angrep vil kunne treffe norske virksomheter.
- Microsoft melder at de har observert de fleste kjente russiske statlige aktører aktive i Ukraina siden krigens utbrudd. Det pågår vedvarende cyberoperasjoner mot ukrainske mål.

HelseCERTs vurdering - Ukraina

HelseCERTs vurdering:

• Vi mener det er lite sannsynlig at norsk helsesektor vil bli utsatt for angrep fra russiske statlige aktører med bakgrunn i krigen i Ukraina.

• 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 med russisk opphav.

• Vi mener det er lite sannsynlig at norsk helsesektor vil treffes av angrep fra hacktivister motivert av krigen i Ukraina. Eksempler på dette kan være tjenestenektangrep.

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. Dette er spesielt viktig for tjenester som e-post og VPN.

4) Kjør HelseCERTs Hurtigtest for cybersikkerhet.

5) Blokker makroer i officedokumenter fra internett.

6) Innfør Microsofts ASR-regler.

7) Innfør applikasjonshvitelisting.

HelseCERTs tilbakeblikk 1.tertial 2022 – Nasjonalt beskyttelsesprogram (NBP)

Norsk helsenett
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.

Vi oppfordrer alle medlemmer til å kjøre Hurtigtest.

https://www.nhn.no/Personvern-og-informasjonssikkerhet/helsecert/nasjonalt-beskyttelsesprogram-nbp

Sårbarhetsskanning

Vi har oppdatert vårt system for skanning slik at vi nå skanner flere domener enn før. Tidligere ble kun domener som førte til en IP-adresse som tilhørte organisasjonen skannet. Nå blir også domener som er registrert under organisasjonen i Norid skannet, uansett IP-adresse. Denne endringen ble gjort for å finne flere sårbare systemer, og samtidig gi informasjon om hvilke domener som ligger under organisasjonens ansvar.

Mange vil derfor se en økning i antall sårbarheter i statistikken som kommer på de neste sidene.

NBP - Tjenester

- Sårbarhetsskanning
- Informasjonsdeling og forebygging
- Hendelseshåndtering
- Blokkeringslister
- Varsling om passord på avveie
- Statusrapport for e-postsikkerhet
- Portskanning
- Webinarer
- Inntrengingstesting
- Hurtigtest

Ta kontakt på post@helsecert.no

For mer informasjon: helsecert.no

Hendelser

- Datainnbrudd hos Helse Nord – det ble avdekket skadevare på enheter som benyttes i ambulanser og luftambulanser hos flere helseforetak. https://helse-nord.no/nyheter/datainnbrudd-i-ambulanser
- Leverandør i sektoren har blitt kompromittert og e-post med ondsinnet kode har blitt sendt ut til en rekke kunder. Vi har bistått med håndtering og oppfølging mot kunder. Lukking av kjente sårbarheter vil redusere risiko for slike hendelser.

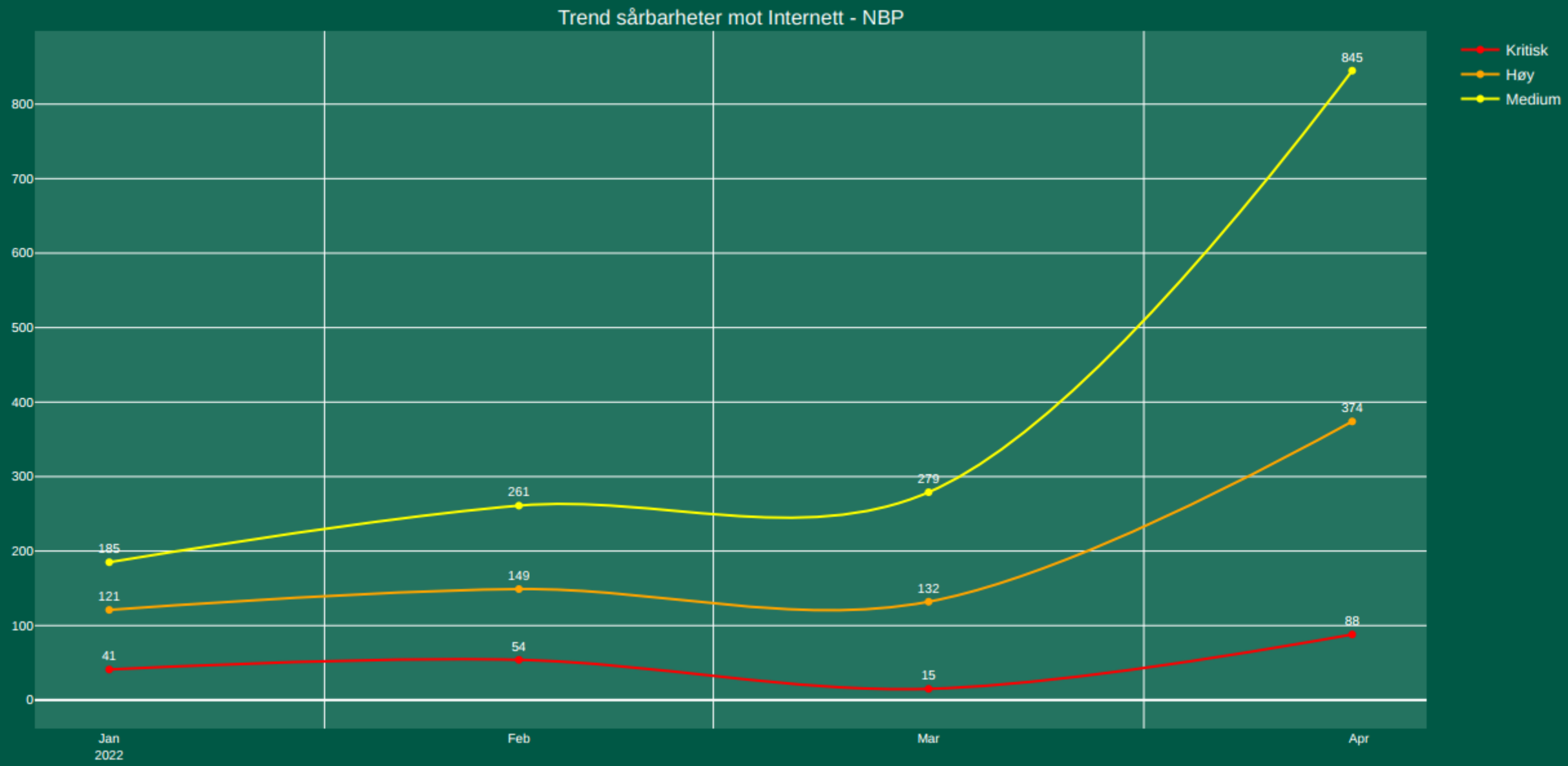
Webinarer

Vi har i 1. tertial holdt 4 webinarer med tema "Multifaktorautentisering", "HelseCERT Hurtigtest", "Tilbakeblikk 2021" og "Passordmanagere".

Opptak av alle webinarer kan sees på https://www.nhn.no/Personvern-og-informasjonssikkerhet/helsecert/nasjonalt-beskyttelsesprogram-nbp/webinarer

HelseCERTs tilbakeblikk 1.tertial 2022 – Statistikk for hele NBP

Norsk helsenett
HelseCERT

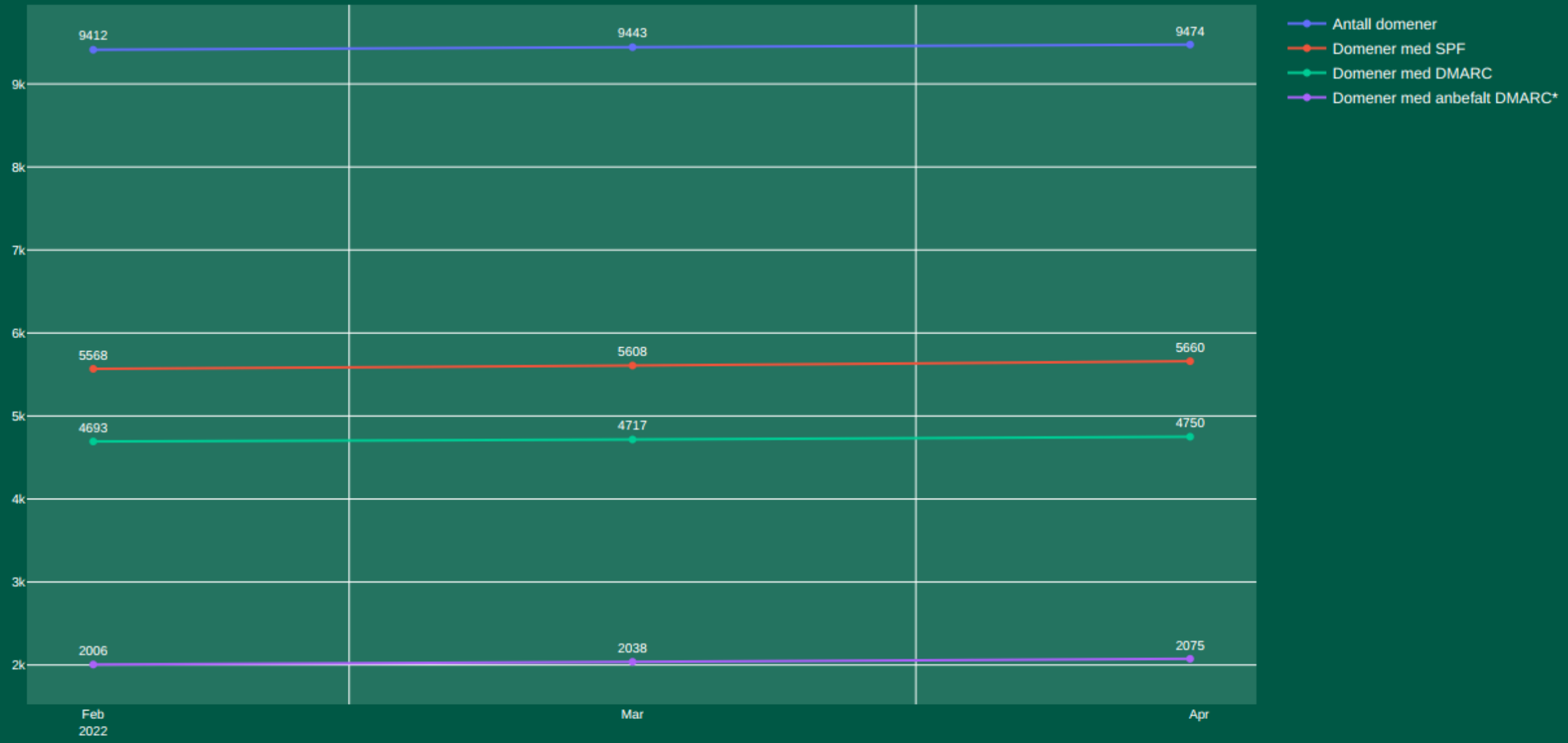


Økningen i april skyldes hovedsaklig endring i skanningen.
Se side 3 for mer informasjon

HelseCERTs tilbakeblikk 1.tertial 2022 – Statistikk for hele NBP

Norsk helsenett
HelseCERT

Trend status for e-postsikkerhet - NBP



* Hvor DMARC policy er satt til «p=reject»
Loggdata for januar er ikke tilgjengelig i denne rapporten

Norsk helsenett

HelseCERTs tilbakeblikk

HelseCERT

Spørsmål og kommentarer kan sendes til
post@helsecert.no
Web helsecert.no