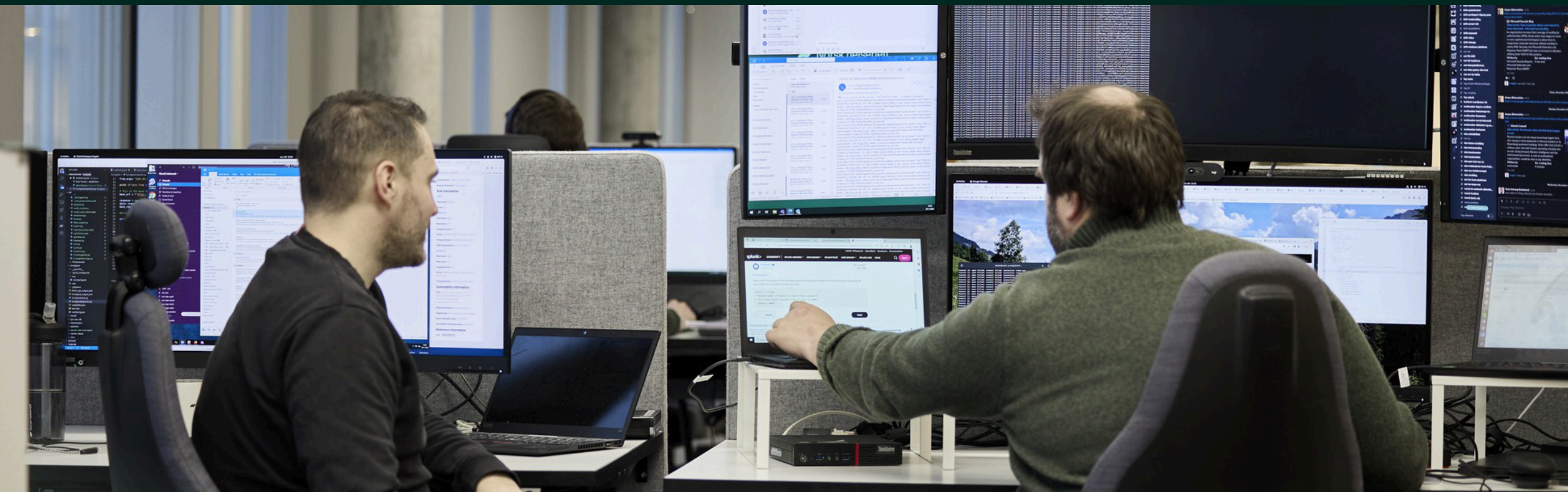
Norsk helsenett

Helse- og KommuneCERT
Tilbakeblikk 1. tertial 2025



Nytt fra Helse- og KommuneCERT

Blokkeringslister v3

Blokkeringslistene (IP-hvitelistet lenke) har fått støtte for følgende i 2025:
- IPv6-adresser som bør blokkeres (*type=ipv6, type=ipv6_cidr)*
- Eget valg for indikatorer som kun bør blokkeres på autentiseringsendepunkter for brukere, f.eks. proxyer, hostingprovidere, VPN-leverandører m.m. (*list_name=auth)*
- Hash for enkel sjekk om listen har endret seg (*hash=md5)*
- Økt ytelse: Last helst ned listen hvert 5. minutt, minst hver time

Listene oppdateres jevnlig både manelt og automatisk, og har 8000+ innslag. De vil aldri kunne ta alt, men tar det vi finner.

Vi har fått god hjelp av medlemmene våre og har scripts og guides
- For blokkering i conditional access
- For blokkering i defender for endpoint
- Listene fungerer også for ordinære brannmur/dns/proxy-løsninger

Fungerer den ikke for din virksomhets løsning? Ta kontakt på post@helsecert.no!

Hurtigtest

Vi har oppdatert Hurtigtest, vår automatiserte sikkerhetstest.

Nå leter den etter flere av svakhetene vi ofte finner i kommunetester, i tillegg til flere andre forbedringer.

Hurtigtest bør kjøres minst tre ganger i året. Om dette gjøres i april, august og desember blir de oppdaterte resultatene med i tilbakeblikk-rapporten fra oss.

Full endringslogg

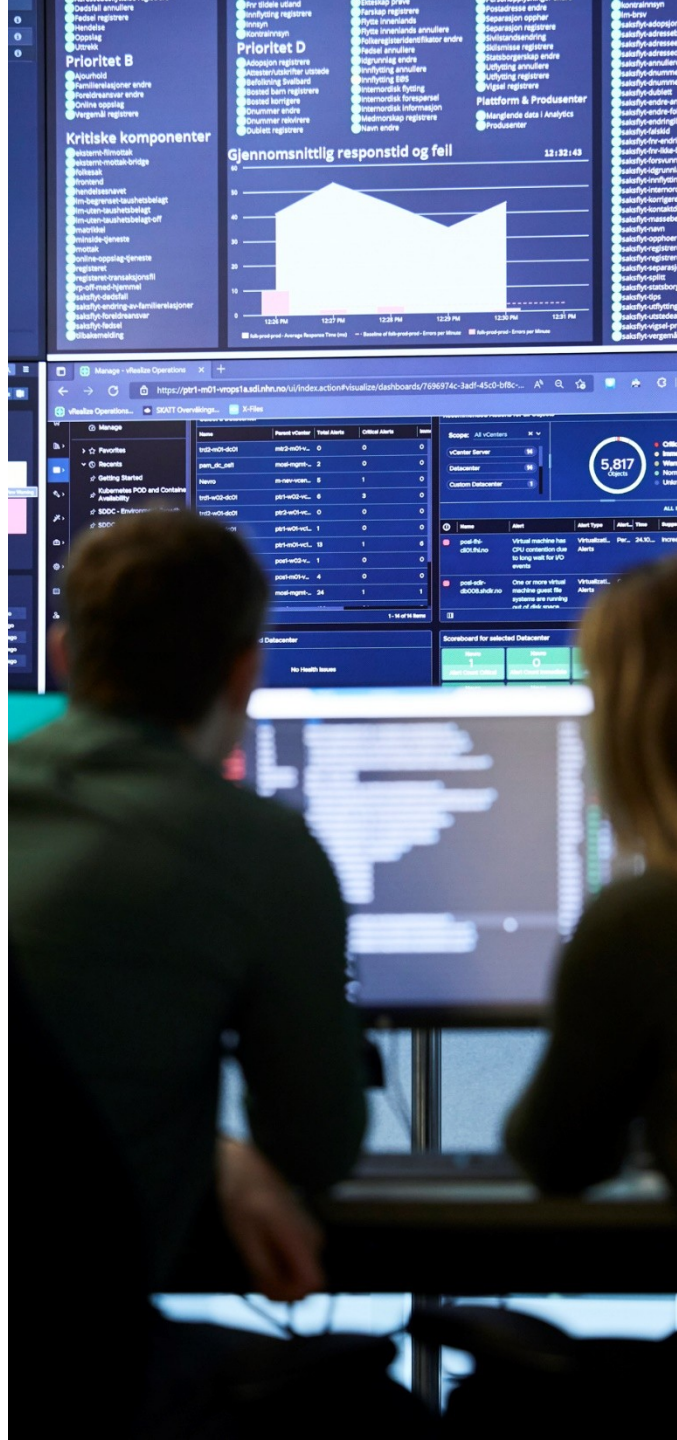
Brukernavn og passord på avveie

Passord på avveie (PPA) brukes som inngangsvektor i angrep. Passord kommer på avveie blant annet gjennom phishing, innbrudd hos tredjepartsleverandører og gjennom skadevare laget for å stjele informasjon. I løpet av tertialet har vi økt tilfanget på slik informasjon vesentlig, og vi jobber aktivt med å få tilgang på mer. NB! Tjenesten garanterer ikke å fange alle passord som kommer på avveie. Det vil alltid være en rest som ikke blir plukket opp. Det er derfor viktig at dere ikke baserer sikkerheten deres kun på denne tjenesten, men bruker den som et tillegg.

Vi varsler medlemmer ved funn på daglig basis. Her ser vi etter innslag hvor vi kan enten kan knytte brukernavnet eller tjenesten til dere. For eksempel hvis brukernavnet er kari.nordmann@helsecert.no vil innslaget kobles til oss. Det samme gjelder hvis innslaget er knyttet til tjenesten https://tjeneste.helsecert.no. Noen ganger kommer vi bare over brukernavn og passord, andre ganger brukernavn, passord, tjeneste og annen meta-informasjon.

Relevante tiltak ved varsling fra oss:
- endre passord som er i bruk hos dere om brukerkontoen fortsatt er aktiv
- varsle berørte brukere så de kan endre passord om det er brukt andre plasser
- identifiser og rydd opp infisert maskin ved skadevare

Det er ikke uvanlig at vi sender ut 500 passord på avveie til medlemmene våre i løpet av en uke.



Angriper i sving

I desember i fjor oppdaget Gran kommune at de var utsatt for at dataangrep. De varslet oss for en vurdering av omfang, og leide deretter inn Defendable for håndtering. De var tilbake i vanlig drift i januar 2025. Hendelsen hos Gran startet med en sårbarhet i internetteksponert programvare, og ville nok endt i ransomware uten rask og besluttsom håndtering straks angrepet ble oppdaget.

Vi har i sist tertial hatt flere webinarer om hendelsen. Først en teknisk og operativ gjennomgang, etterfulgt av en gjennomgang av administrativ håndtering på kommunalt nivå. Påfølgende webinar om sentralisering av AV-logger, og deretter om loggsikring i en hendelse er inspirert av hendelsen. Gran kommune valgte å ta ned mange tjenester i forbindelse med håndtering av hendelsen. Nedetid på tjenester var også den største konsekvensen for kommunen.

Vi ble tidlig kontaktet og har hatt et bra samarbeid med Gran både under og etter hendelsen. De har hele veien vært åpne og delt raust av egne erfaringer. Vi takker de for godt samarbeid og en forbilledlig delingskultur!

Læringspunkter vi ønsker å framheve

- Viktigheten av å holde internetteksponerte enheter **oppdatert**
- Det å **samle inn, og følge opp**, AV-alarmer (spesielt servere)
- Servere bør **ikke kunne koble fritt ut** mot internett
- **AD-tiering** er en viktig on-prem sikringsmetode (Se egen side i tilbakeblikk, og webinarserie i mai/juni 2025)

AD-tiering

En kjent svakhet i Windows-miljøer er at passord-hasher kan hentes ut av minnet og gjenbrukes i angrep. Om angriper kommer på en maskin hvor en administrator har vært innlogget, kan de på denne måten gå fra vanlig bruker til administrator.

Vår erfaring fra hendelser og kommunetester er at dette er et stort problem.

Vi anbefaler derfor AD-tiering, som går ut på å ha dedikerte brukere for administrasjon av klienter, servere og domenekontrollere, og å passe på at disse brukerne ikke blandes. Det gjør det umulig å få tak i passord-hashen til domeneadministrator fra en klientmaskin.

AD-tiering er et gratis og viktig sikringstiltak. Vi vil ha fokus på dette i tiden framover, blant annet gjennom egne webinarer i mai/juni.

AD-tiering er spesielt relevant i on-prem miljøer, noe mange av våre medlemmer har.

Anbefaling – phishingresistent autentisering

Vi anbefaler å kreve

- Innrullerte enheter eller **Passnøkler** eller **Windows Hello for Business** eller **Sertifikatbasert autentisering**

Betinget tilgang, conditional access på engelsk, går ut på å kombinere forskjellige faktorer for å vurdere om en innlogging skal godtas eller ikke. Slike faktorer kan være passnøkler, passord, sertifikat fra innrullert enhet, hvor innlogging kommer fra (IP-adresse), om enheten er registrert med mer.

Se vår anbefalingsside med herdeguider for å kombinere slike faktorer.

Hva annet kan gjøres?

1. Krev registrerte enheter. (Se eget webinar). Gir samme beskyttelse mot phishing som krav om innrullerte enheter, men gir ikke kontroll på enheten.
2. Bruk en/flere av metodene under for å redusere risiko. Merk at dette ikke er fullgode løsninger, men er mye bedre enn å ikke gjøre noe.
    - Begrens mulighet for innlogging fra ikke-innrullerte enheter til kun norske adresser (lokasjonsbasert /geoblokkering)
    - Bruk våre blokkeringslister i conditional access (IP-adressebasert – NB! Merk at det også ligger hele IP-nett her, og ikke glem å hente inn IPv6-delen av listene som tilbys i blocklist v3)
    - Benytt risky users / risky sigins. Om lisensnivået deres støtter det, kan Microsofts deteksjon brukes til dette. Vi opplever at denne tar mye, men kjenner til flere tilfeller av kompromitteringer blant våre medlemmer hvor pålogging ikke har blitt flagget. Det er derfor svært viktig at dette ikke er eneste tiltak.

Etterhvert som de ulike phishing-kittene/tjenestene benytter proxyer som simulerer/imiterer offerets lokasjon (omtalt som residential proxies) vil metodene under pkt 2 miste effekt. I praksis vil innloggingene se ut som de kommer fra tilfeldige norske hjemme-IPer. De færreste phishing-kit/tjenester benytter det i dag men vi har sett flere angrep med det. Vi forventer at dette kommer mer framover.

- **OBS**: Bruk av passord + multifaktorautentisering er sårbart for phishing og er derfor ikke godt nok. Slike angrep er beskrevet i eget webinar.
    - Se også vårt webinar om phishingresistent autentisering

Innrullert enhet / Compliant device vil si en enhet som er administrert av virksomheten, eksempelvis via Intune eller tilsvarende mekanismer.

- En vanlig felle er å krever innrullert enhet for bruk av applikasjoner (Teams, Outlook) men tillate innlogging fra nettleser på ikke-innrullerte enheter for å støtte Bring Your Own Device (BYOD). I dette tilfellet må man bruke passnøkler eller kreve registrerte enheter.
- **Det er innlogging via nettleser som angriperne gjør.**
- Det er viktig å ha en solid prosess for innrullering av enhetene, her kan samme mekanismer som vi omtaler under webinar for å kreve registrerte enheter benyttes. Vi forventer at phishing av selve innrulleringsprosessen vil komme i løpet av året.

Passnøkler

- Faller inn under det Microsoft definerer som phishingresistent autentisering
- Kan gjøres både i programvare og maskinvare (FIDO-nøkler)
- Gir en vesentlig bedre brukeropplevelse enn ordinær multifaktorautentisering.

Brukernavn og passord på avveie – NBP

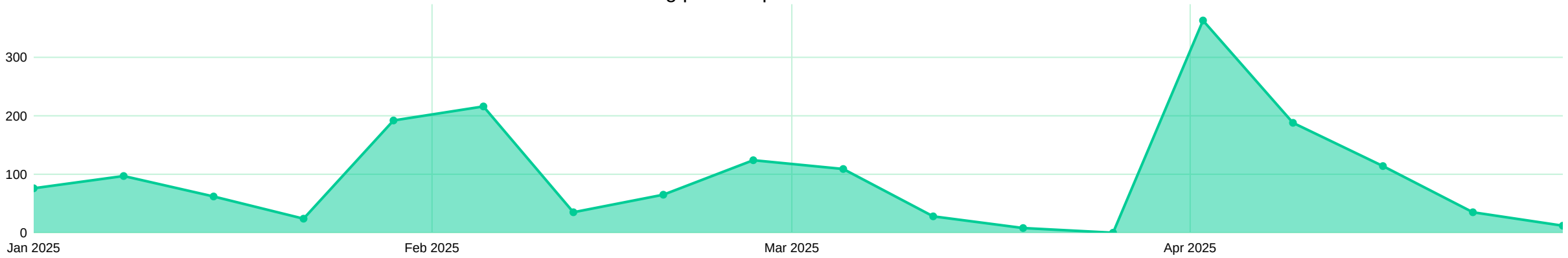
Antall brukere varslet om passord på avveie første tertial 2025

41.3k

Antall varsler sendt første tertial 2025

1748

Antall varsler om Brukernavn og passord på avveie sendt totalt for NBP i første tertial 2025



Tilbakeblikk 1.tertial 2025

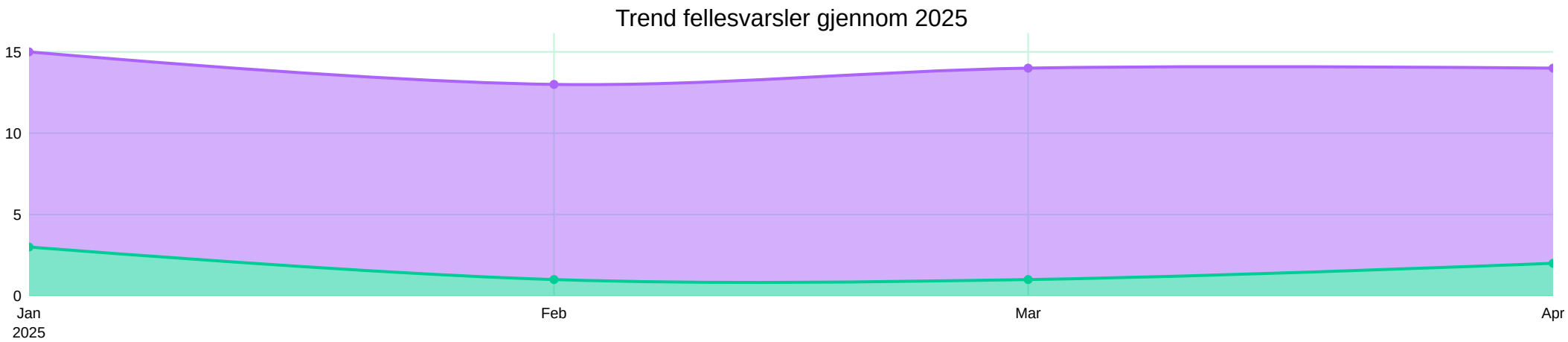
Informasjonsdeling – NBP

Antall fellesvarsler sendt til NBP-saarbarhet-patch gjennom 2025

56

Antall fellesvarsler sendt til NBP-trussel gjennom 2025

7



Tilbakeblikk 1.tertial 2025

Who you gonna call?

Varsle hendelser

- Enten dere ønsker hjelp eller om det er "til info".
- Hendelser kan være
  - Forsøk på svindel
  - Phishing
  - Skadevare på maskin
  - Angriper i nettverk
- Vi ønsker å hjelpe
- Vi ønsker å vite så vi kan hjelpe andre bedre

Varsling av tidskritisk hendelser:
Ring 24 20 00 00
be om Helse- og KommuneCERT

Varsling av ikke tidskritiske hendelser:
E-post til incidents@helsecert.no

Hvordan melde M365-phishingangrep

Ved å varsle oss om phishingforsøk og annen mistenkelig aktivitet, kan vi bidra til å gjøre både medlemmene og Norge som sådan sikrere gjennom effektiv informasjonsdeling. Vi ber om at dere sender oss følgende informasjon:

- Avsenderadressen
- Phishing-lenken i den originale e-posten
- Kopi av den originale phishing-e-posten (som vedlegg)
- IP-adresser angriper logger inn fra
- User-Agent(s) angriper bruker
- Tidspunkt for e-post og for innlogging
- Hva angriper har gjort med tilgang

Vi setter pris på all informasjon dere kan sende oss, selv om dere ikke har mulighet til å dekke alle punktene.

Rapporter via rapporteringsskjema eller til post@helsecert.no.

Norsk helsenett

Helse- og KommuneCERT

Tilbakeblikk 1. tertial 2025

post@helsecert.no

Har du forslag til hvordan tilbakeblikk kan bli bedre? Skann QR-kode og hjelp oss. Eller bruk link.
De går samme plass.