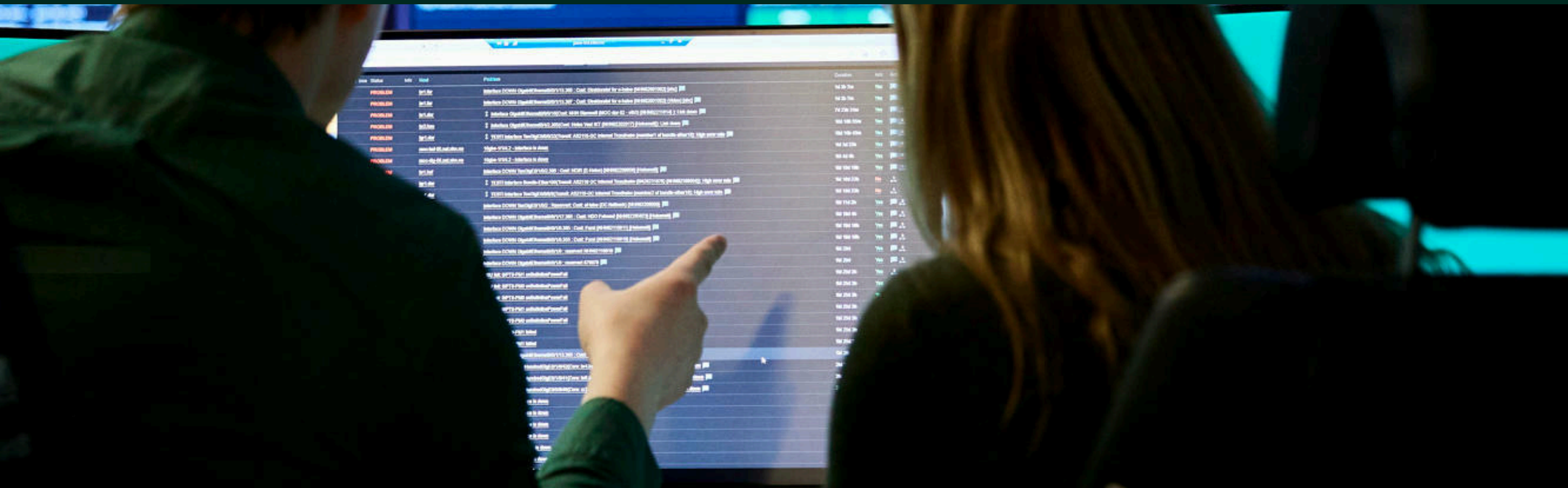
Tilbakeblikk 1. tertial 2026
Helse- og kommunesektoren



Innholdsfortegnelse

♻️ Tilbakeblikk er laget for digital lesing og er inndelt etter tema, ikke A4-størrelse. ♻️

Nytt fra Helse- og kommuneCERT

OT-sikkerhet

Vi har fortsatt et økt fokus på sikkerhet inn mot operasjonell tekonologi (OT) og vann og avløp (VA).

I løpet av de siste månedene har vi gjennomført sikkerhetsvurderinger av flere kommunale vannverk. I juni kommer et webinar med hvilke erfaringer disse vurderingene har gitt. Nærmere informasjon og invitasjon til webinaret vil bli sendt ut til e-postlistene NBP-info og NBP-VA.

I tillegg hadde vi i januar ett fokus på å identifisere og varsle virksomheter i sektoren om OT-systemer direkte eksponert på internett. Gjennom arbeidet avdekket vi og varslet medlemmer om flere styringssystemer, industrielle rutere med svakheter, og operasjonelle protokoller som ikke skal eksponeres direkte på internett.

Kartlegging av OT-relaterte systemer på internett er fortsatt et fokus for oss i tiden fremover. Dersom din virksomhet har IP-adresser og domener tilknyttet OT som er eksponert mot internett, er det fint om disse sendes til oss. På denne måten kan vi gjøre mer presise undersøkelser. Informasjon kan lastes opp i vår medlemsportal.

Vi har i første tertial også sendt ut flere varsler til NBP-VA med anbefalinger knyttet til sikring av OT. Varslene har tatt for seg ulike deler av vår OT-sjekk.

Varslene er tilgjengelig i artikkelform på våre nettsider:

- OT-systemer eksponert på internett
- Utstyrsoversikt, ansvar og rutiner
- Oppdatering, sikkerhetskopiering og utfasing av operasjonell teknologi
- Passord og nettverkssegmentering i operasjonell teknologi
- Overvåkning og logging i OT-nettverk

Hurtigtest

Hurtigtest versjon 8.2 ble lansert 7. mai, med to nye sjekker og forbedringer på eksisterende.

I tillegg vil Hurtigtest-funn nå vises på herdingssiden deres i portal, og hurtigtest inngår nå som en del av herdingsløpet.

Vi anbefaler at hurtigtest kjøres minimum tre ganger i året. Full endringslogg

Blokkeringslistene

Blocklist-tjenesten er nå tilgjengelig på for nedlasting via både IPv4 og IPv6.

- blocklist.helsecert.no for bruk over IPv4
- blocklist6.helsecert.no for bruk over IPv6

Endringen tredde i kraft torsdag 7. mai 2026.

Det er kun IPv4-adressen som har statisk IP. 20.251.240.3

blocklist6.helsecert.no har dynamsik IP-adresse.

Medlemsherding

Medlemsherding baserer seg på flere verktøy. I dag bruker vi PingCastle sammen med egenutviklede Hurtigtest og Skytest.

Mens sårbarhetsskanningen vår ser på hvor godt sikret dere er fra utsiden, vurderer Medlemsherding hvor robust AD-miljøet på innsiden er. Dette samsvarer direkte med om, eller hvor fort, en løsepengevirusaktør fullfører angrepet om de først har fotfeste.

For å sitere tidligere sjef FBI, Robert Mueller, «… there are only two types of companies: those that have been hacked and those that will be» RSA Cyber Security Conference, 01. mars 2012.

Med det som utgangspunkt vil trusselaktører få fotfeste hos dere på et eller annet punkt. Medlemsherding sørger for at dette fotfestet ikke blir til store tap.

Vi anbefaler alle medlemmer å gjennomføre et herdingsløp via portal.helsecert.no. Dette vil øke motstandsdyktighet mot framtidige angrep. Gjennomført herdingsløp kvalifiserer dere også til å bestille en gratis inntregningstest hos oss.

Device code phishing-angrep

Vi har sett en kraftig økning i device code phishing-angrep. Dette er en type AiTM-phishing der angriperne lurer brukere til å godkjenne en «device code» fra Microsoft, og dermed får tilgang til kontoen via OAuth-tokens.

Viktig å vite:

Angriperne får tilgang, men får ikke passordet. Derfor dukker dette heller ikke opp i Passord-På-Avveie-tjenesten vår.

Hva gjør angriperne med tilgangen?

De bruker Graph API og henter ut informasjon, som stillingstittel. De bruker nøkkelord for å søke etter sensitiv informasjon i innbokser. De bruker AI for å identifisere hvilke e-post-tråder som er mest verdifulle å koble seg på, med mål om å få ut mest mulig penger med svindel.

Hva bør du gjøre?

Device code phishing er enkelt å blokkere for. Se guide 5 https://www.nhn.no/tjenester/helsecert/nasjonalt-beskyttelsesprogram-nbp/anbefalte-sikkerhetstiltak/autentisering/brukerguides-for-m365-conditional-access

Vi har også et webinar om device code phishing, se opptak og info her: https://www.nhn.no/tjenester/helsecert/nasjonalt-beskyttelsesprogram-nbp/webinarer

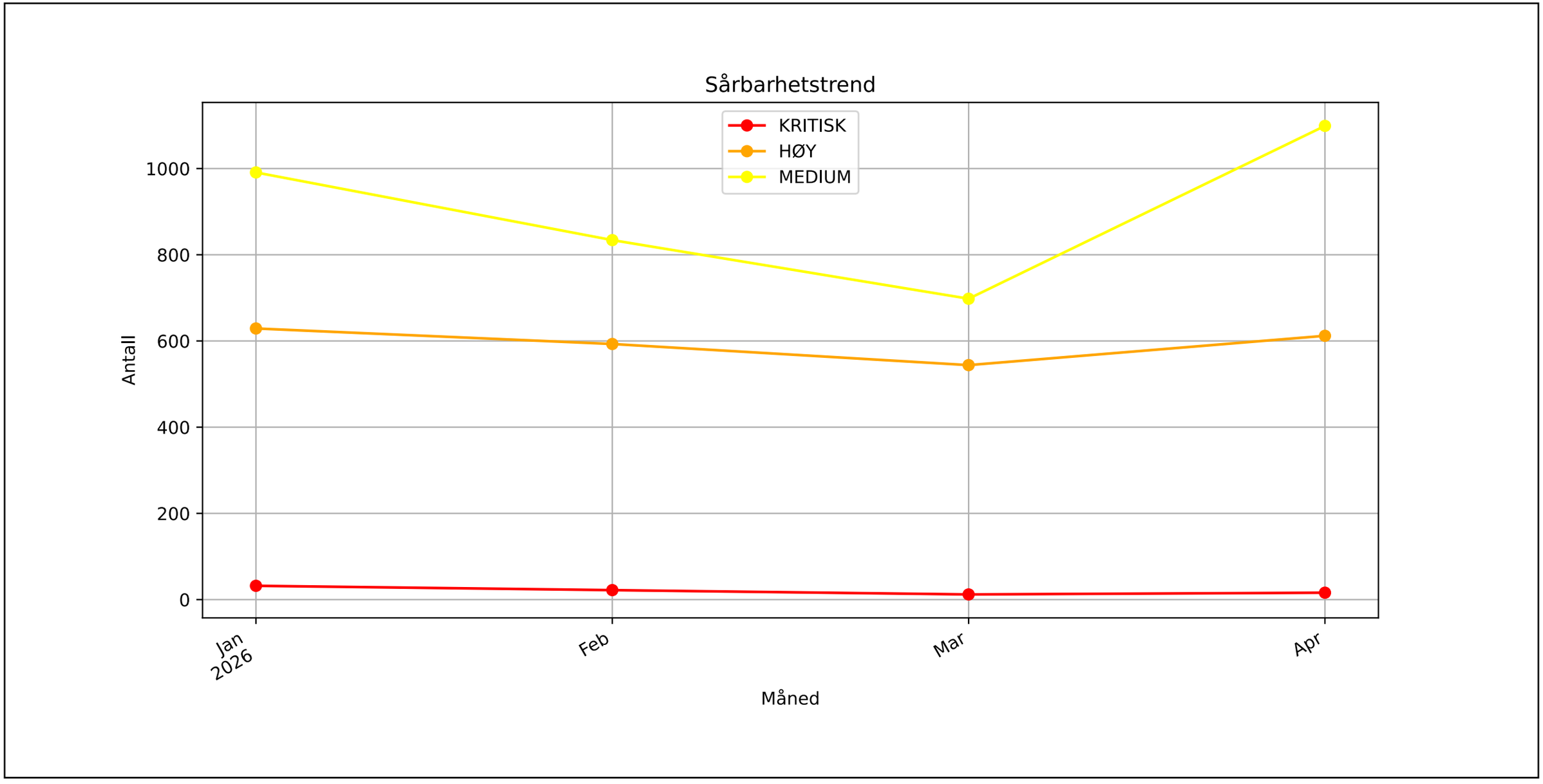
Skytest

Skytest versjon 1.4 ble lansert 7. mai, med en rekke nye sjekker.

I tillegg vil Skytest-funn nå vises på herdingssiden deres i portal, og er en del av herdingsløpet.

Vi anbefaler at skytest kjøres minimum tre ganger i året. Full endringslogg

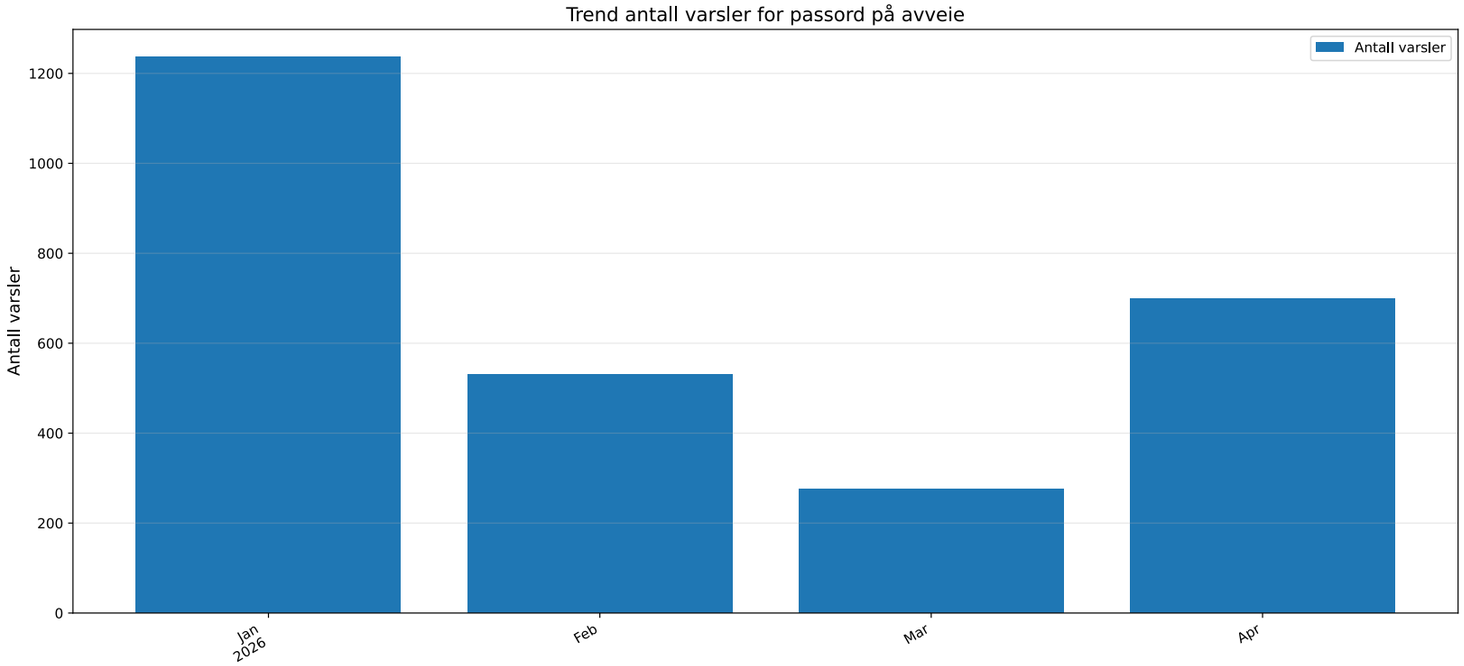
Sårbarhetstrend for NBP

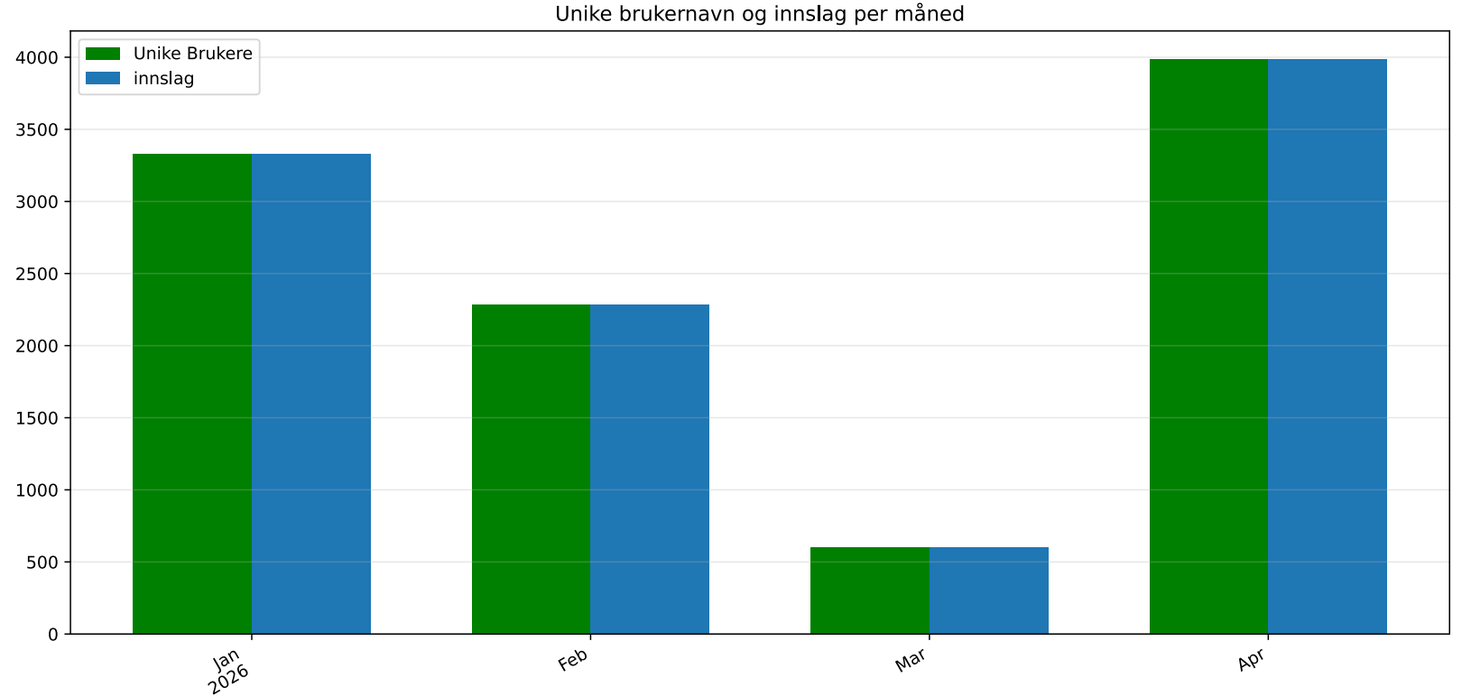


Det foregår til enhver tid mye skanning etter kjente sårbarheter. Noe av dette gjøres av aktører med gode hensikter, skanneren vår er et eksempel på dette. Annet kommer fra angripere, og oppdager de sårbarheter ender det i verste fall med ransomware.

Tiden fra sårbarheter blir kjent til de blir utnyttet er i mange tilfeller svært knapp.

Aggregert brukernavn og passord på avveie-statistikk





Innlogginger sikret kun med brukernavn og passord er en stor kilde til cyberangrep. Det er store mengder brukernavn og passord tilgjengelig åpent, og for salg på det mørke nettet. Slike passord kommer fra blant annet phishing, stealere (skadevare som stjeler passord) og kompromitterte nettsider (f.eks. LinkedIn i 2012).

Tjenesten vår «Brukernavn og passord på avveie» samler inn det vi finner gjennom samarbeidspartnere. Vi fjerner duplikater og sender info videre til dere så dere kan gjøre tiltak. Her ser dere litt grafer over hvor mye som er varslet for 2026. Datapunktene er aggregert per måned.

Du kan lese mer om tjenesten på nettsidene våre.

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 tidskritiske hendelser:
Ring 24 20 00 00
be om Helse- og kommuneCERT

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