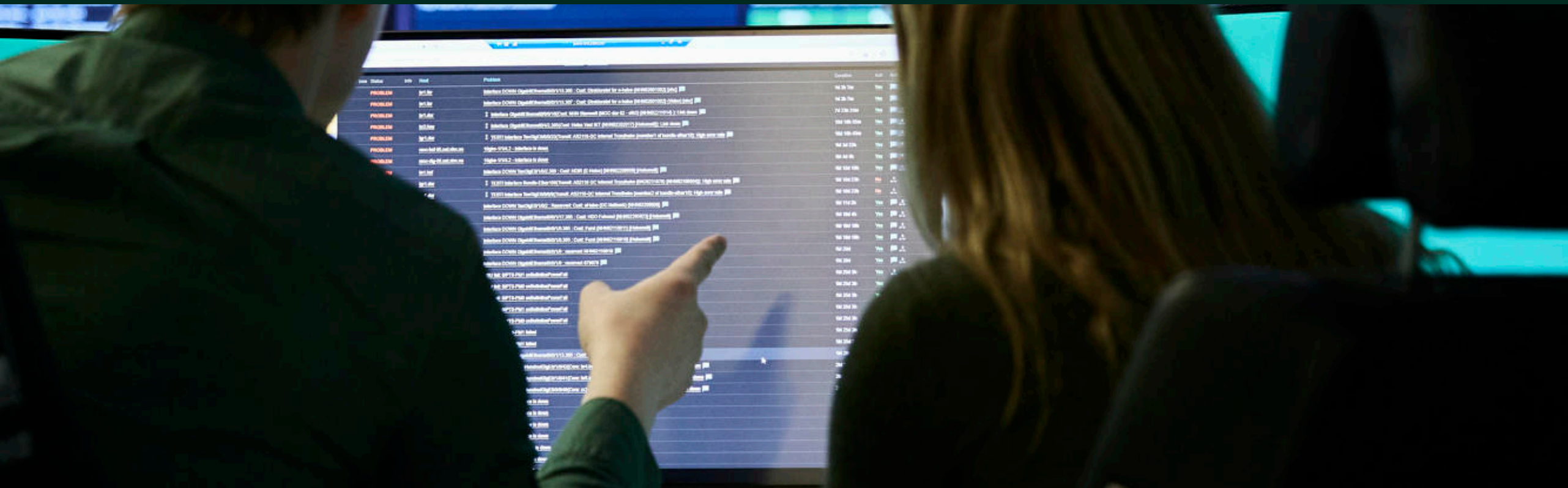
Tilbakeblikk 3. tertial 2025
Helse- og kommunesektoren



Innholdsfortegnelse

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

Nytt fra Helse- og kommuneCERT

Skytest

I november hadde vi lanseringswebinar av Skytest. Skytest er et audit verktøy for Entra ID, Azure og InTune. Verktøyet gir en oversikt over konfigurasjoner og sikkerhetsinnstillinger.

De vanligste feilkonfigurasjonene har tilhørende guider for fiksing.

Skytest kan lastes ned fra portal.helsecert.no (krever at man har opprettet bruker, og at virksomheten man jobber i er medlem hos oss).

Tilbakeblikk sier ifra om Skytest er lastet ned og kjørt. Vi anbefaler at alle gjør det en gang i tertialet og utbedrer eventuelle funn. Ved problemer, ta kontakt med oss på post@helsecert.no.

Blokkeringslistene

Vi tilbyr blokkeringslister med IP-adresser og domener brukt i angrep. Alle innslag er ting vi finner selv, får fra medlemmer, eller fra partnere vi stoler på.

Listene oppdateres jevnlig både manuelt og automatisk, og har i dag 22000+ domener og 1400+ IP-nett. De vil aldri kunne ta alt, og de er ikke en erstatning for evt kommersielle lister. Listene er likevel et godt tillegg til andre mekanismer, og vi vet at de i flere tilfeller har forhindret angrep.

Listene kan brukes i brannmurer, proxy, DNS-servere, Defender for Endpoint og Entra ID, for å nevne noen. Skripts og guider for å komme i gang er tilgjengelig på github.

- Guide for blokkering i Conditional Access i Entra ID
- Guide for blokkering i Defender for Endpoint (Eksempelet er for annen datakilde, konseptet er likt)

De fleste av skriptene kommer fra medlemmer. Takk! Har dere skript eller guide for implementasjon hos dere og den ikke ligger på github-siden vår? Ta kontakt med oss på post@helsecert.no!

Verdt å være klar over for blokkeringlistene:

Subdomener: Alle subdomener av domener i blokkeringslisten skal blokkeres

Blokkeringslistene blokkerer kun høyeste nivå av domene. Hvis vi i vårt system/automatikk legger inn både `test.example.com` og `example.com` så vil blokkeringslistene kun publisere `example.com`. Det betyr at mekanismen som konsumerer blokkeringslistene må settes opp slik at `test.example.com` også blokkeres. Vi ser en del angripere bruke tilfeldige subdomener i kampanjene sine.

Hvis blokkeringsmekanismen man har krever at blokkeringslisten oppgir `*.<domene>`, så kan man legge til `&type=wildcard_domain` som parameter i API-spørringen. Dette vil returnere samtlige innslag av typen `domain`, men med `*.` foran. Dette er tilfelle for eksempelvis Fortigate-brannmurer.

Listene har mange oppføringer

Om man har en grense for hvor mange innslag løsningen kan ta imot, kan man oppgi en grense: Bruk parameter `limit`.

Tiltenkt bruk for IP-baserte lister - `default` vs `auth`

- **Brannmur/proxy/endepunktsløsninger**: Hindre at enheter hos dere **kobler ut** til angrepsinfrastruktur. Denne listen kaller vi `default`, og man trenger ikke å presisere listenavn for denne typen løsninger - `list_name=default` er et implisitt parameter.
- **Autentiseringsløsninger** (Entra ID, VPN pålogging, …): Hindre **påloggінger** fra både kjente angreps-IPer og IP-adresser vi forventer at angripere vil koble til fra, for eksempel kommersielle **VPN-tilbydere**, **hosting-leverandører** med mer. For autentiseringsendepunkter så anbefaler vi at dere bruker `list_name=auth&list_name=default` i API-spørringen.

Flere av IP-adressene i blokkeringslisten kan man forvente å se både utkoblinger *til* og autentiseringsforsøk *fra*. Dette gjelder spesielt IP-adresser benyttet i AitM-phishing.

Listene er robuste

Det er ikke noe problem å oppdatere listene ofte. Vi anbefaler at man sjekker etter oppdateringer hvert 5. minutt.

Ideelt sett bruker alle medlemmer blokkeringslistene våre både på perimeter, endepunkt og for innlogging

OT-sikkerhet

Vi har den siste tiden hatt økt fokus på VA-sikkerhet. (VA=Vann og avløp). De fleste prosesser der er innenfor Operasjonell teknologi (OT). Forskjell en mellom IT og OT er at mens IT styrer og holder på informasjon styrer OT (operasjonell teknologi) fysiske prosesser. Som en del av dette fokuset har vi funnet og varslet om mange hundre OT-systemer rett på internett, holdt webinar om OT-sikkerhet 101, gitt ut anbefaliner for OT-sikkerhet gjennomført sikkerhetstester av flere vannverk og gitt ut flere temarapporter:

Oppdatering og utfasing av OT-utstyr - OT-systemer eksponert på internett Utstyroversikt for OT

Temarapportene sendes ut på den nye e-postlisten vår nbp-va (Vann- og avløp). Ta kontakt om du vil legges til på listen: post@helsecert.no

Medlemsportal

I 2025 begynnte vi å jobbe med en medlemsportal. Vi utvikler den fortsatt videre, men per nå kan man bruke den til:

- Laste ned hurtigtest og skytest.
- Bestille pentest (tidligere kalt kommunetest).
- Se egen registrert nettverksinformasjon (hvile domener og IPer vi har registrert på dere)
- Se hvem hos dere som står på mailinglister hos oss
- Se og endre på informasjon knyttet til VA hos dere
- Se en stor mengde kunnskapsartikler om herding

Bruker kan opprettes av den enkelte. Bruker bør benytte jobb-epost, og første innlogging må skje med ID-porten, (MinID, Bank-ID, Buypass, Commfides). Deretter kan man opprette en (♥phishingresistent♥) passnøkkel for senere innlogginger.

Gruppeadministrator er en av dere som har rettigheter til å styre hvem hos dere som har tilgang til hva. F.eks. kan man skru på at andre brukere har, eller ikke har, tilgang til å laste ned hurtigtest. En administrator kan heve andre til administrator.

Vi jobber stadig med å få inn nyttig funksjonalitet i portalen. Logg gjerne inn og se dere rundt på portal.helsecert.no. Kommer dere over feil hører vi gjerne om det på post@helsecert.no

Forbedringer i portskannrapport

Portskannrapporten er forbedret med følgende:

- Domener vi antar kan slettes er nå tydelig markert (NX-domains)
- Porter med falske positiver er filtrert i egen fane

Hvordan vi tenker portskannrapport kan brukes

- Som en oversikt over deres internetteksponering
- For å jevnlig gå over at det som ligger åpent skal gjøre det.

Har du tilbakemeldinger for hvordan portskannrapporten kan bli bedre? Ta kontakt på post@helsecert.no!

Angrepsflate

Angrepsflate

I desember hadde vi to sårbarhetshendelser [1] som illustrerer viktigheten av reduksjon av angrepsflate. Altså å fjerne åpninger og tjenester som ikke trenger å stå på nett, eller som kanskje ikke trengs lengre i det hele tatt.

MongoDB

Kritisk sårbarhet på julaften kan oppfattes suboptimalt. Vi fanget denne opp 25. desember, og vakten begynte med en vurdering. MongoDB er en database, og her er det lett å tenke at dette er det ingen som setter rett på internett. Det var det 130 000 som hadde gjort. Heldigvis var kun 29 av disse i Norge. Ingen medlemmer av oss var ansvarlige for noen av disse, noe som gledet oss veldig, både på grunn av tidspunktet, og rent generelt. Her har dere gjort en god jobb med å begrense egen angrepsflate. Dette gjorde at ingen fikk en telefon fra oss 25. desember med budskap «du må gjøre noe NÅ», og vakten vår avsluttet arbeidet relativt kjapt.

SNMP

I tillegg til sårbarheten i MongoDB, dukket det 26. desember 2025 opp en kritisk sårbarhet i Net-SNMP. SNMP er en protokoll vi lenge har varslet som HØY, selv uten noen kjente sårbarheter. Det er på grunn av tilfeller som dette. SNMP er en protokoll til internt bruk i et nett og har ikke noe på internett å gjøre. Tilfeller som denne er også grunnen til at vi flagger slikt såpass høyt i sårbarhetsskannrapportene dere får, selv uten kjente sårbarheter. Dette er unødvendig angrepsflate hvor sårbarheter kan bli kjent, og utnyttet til ubeleilige tidspunkt.

Styr egen arbeidsflate

Vi avslutter historietimen med en oppfordring: Dere får månedlig en portskannrapport. Formålet med den er å gi dere et godt bilde av hvilken angrepsflate dere eksponerer. Vi ønsker at dere går gjennom portskannrapporten når den kommer og fjerner det dere kan slik at vi fortsetter uten funn.

[1] - Vi omtaler hva sårbarhetshendelser er i forrige tilbakeblikk

Case studie: Residential proxies

Residential proxies

De siste månedene har vi varslet flere av dere om «residential proxies» i egne nettverk. Hva er dette, og hvorfor mener vi at dette er noe dere bør rydde bort?

Hvilket land kom du fra, igjen?

Funksjonen for residential proxies er å gi kunden - altså brukeren av proxy-nettverket - mulighet for å fremstå som om de er en helt ordinær bruker som er lokalisert i et hvilket som helst land. Kunden velger hvilket land hen skal koble ut gjennom. Tenk på det som VPN, bare at det er spesifikt laget for å være ekstra vanskelig å oppdage. Det er ikke markert som proxy eller om man slår opp i for eksempel whois, og det vil som regel se ut som en helt ordinær sluttbruker.

Som regel uønsket

Residential proxy er normalt et stykke programvare man kjører på datamaskiner, telefoner eller smart-enheter (internet of things) som for eksempel digitale bilderammer. I de aller fleste tilfeller kjører dette uten at bruker er klar over det - det har for eksempel kommet inn sammen med annen programvare, eller kan til og med være plantet hos leverandør om man har maks uflaks. Vi kjenner til at det har blitt bundlet med videocodecs, integrert i applikasjoner for deling av videostrømmer, integrert i mobil-apper eller rett og slett er en del av skadevare som blir installert etter kompromittering av enheten/maskinen.

Residential proxies er en bakdør inn i eget nettverk og mot andre i Norge

Residential proxies gir som nevnt enkel tilgang å endre opprinnelsesland for angrep. Flere phishingkits bruker slike nettverk for å utføre phishingangrep, hvor IP som brukes for å logge på Entra ID blir satt til å være mest mulig likt (iallfall samme land, kanskje også samme internettleverandør) som IP-adressen som besøker phishingsiden. Dermed omgår de både geoblokkering og mye automatisk deteksjon. **Ville dine analytikere luktet lunta, hvis de så at innlogging - *kanskje* flagget som mistenkelig - kom fra en norsk hjemme-IP, eller kanskje til og med fra deres eget gjestenett?**

Vi vurderer derfor fortløpende å mate de residential proxies vi kjenner til i Norge inn i blokkeringslistene våre, for å minske sjansen for kompromittering den veien.

Et annet og like alvorlig problem er at residential proxies kan gi tilgang til interne nettverk. Slik kan angripere omgå skallsikring og nå interne, mindre sikrede tjenester. I verste fall kan dette føre til at ransomware-grupper har direktetilgang til interne systemer.

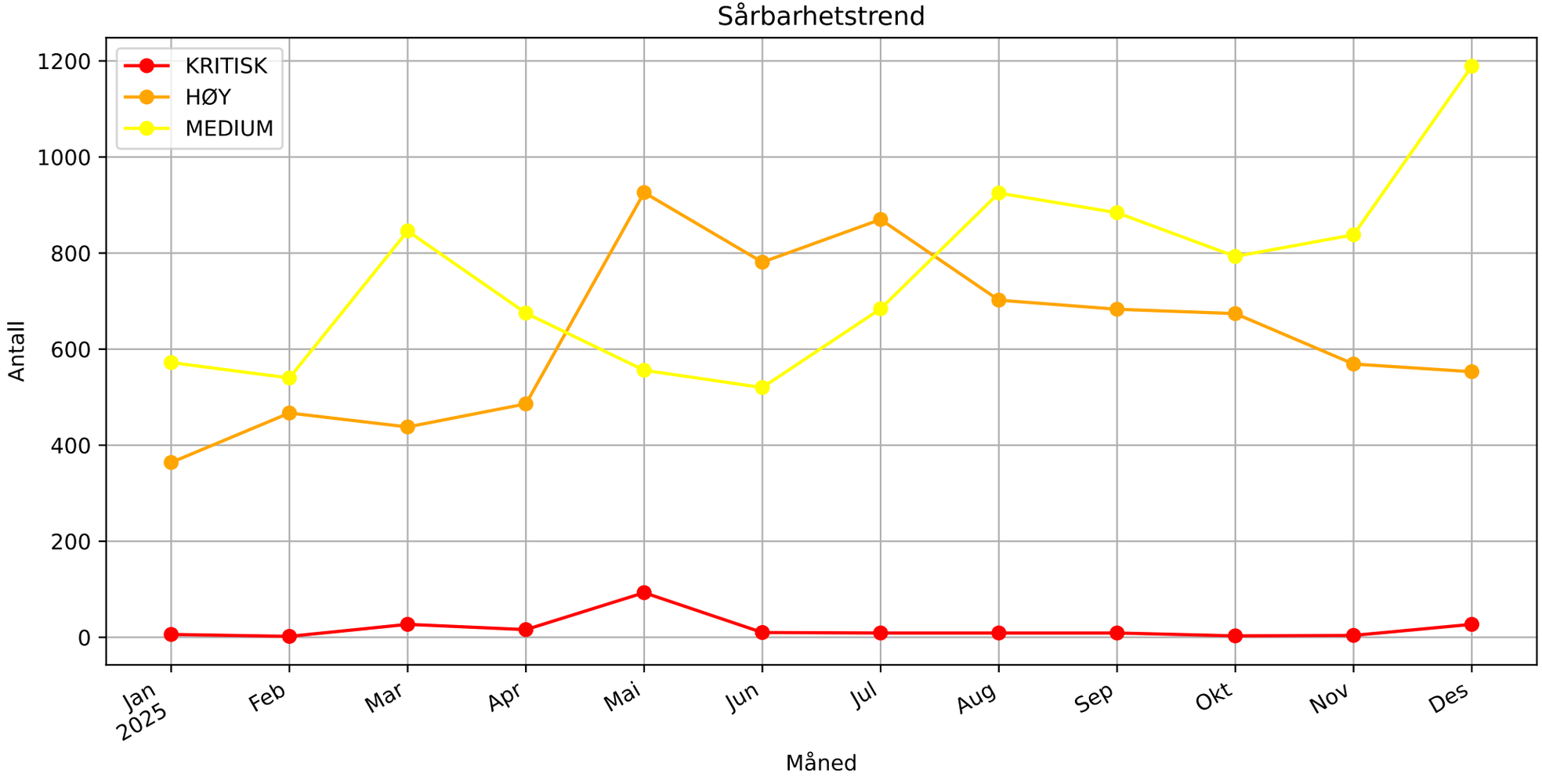
Retningslinjer, applikasjonshvitelisting, rydding

Vi behandler residential proxies som skadevare, og varsler det deretter. Siden det brukes aktivt i angrep blant annet i phishing-kits varsler vi, så langt det lar seg gjøre, også om residential proxies på gjestenettverk.

Vi anbefaler at dere:

- gjennom retningslinjer og tekniske tiltak som applikasjonshvitelisting styrer hva som kan installeres på virksomhetsmaskiner.
- fjerner oppdagede residential proxies, og bistår med opprydning, også på gjestenett
- sørger for sporbarhet på gjestenett og elevnett - det er her vi har funnet de fleste tilfellene av residential proxies blant våre medlemmer
- sørger for at gjestenett har separat offentlig IP-adresse fra resten av virksomheten

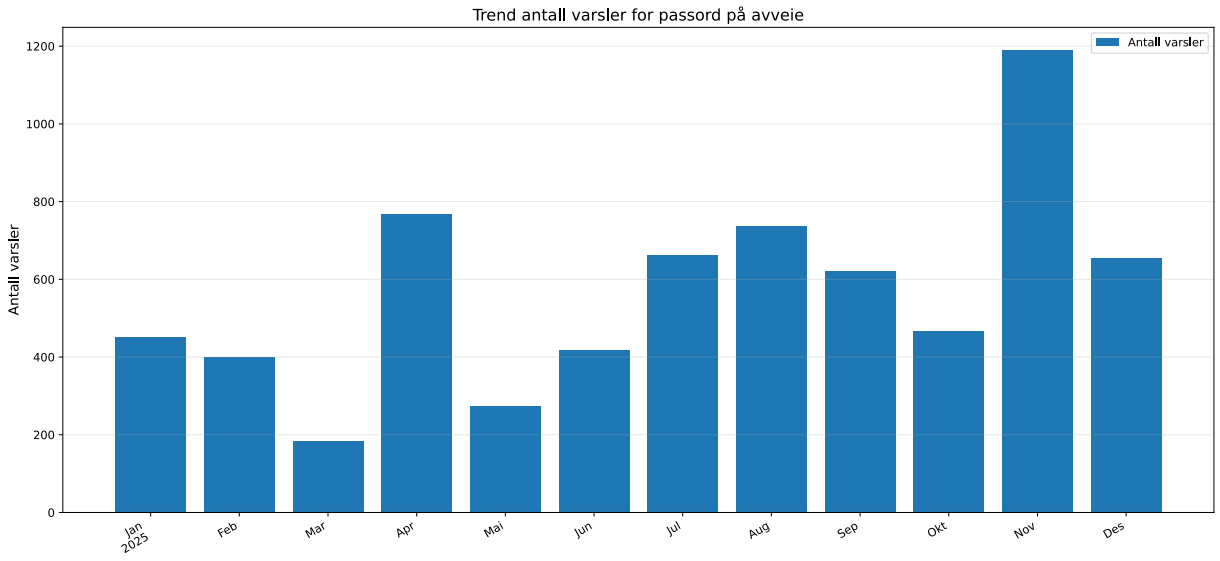
Sårbarhetstrend for helse- og kommunesektoren i NBP

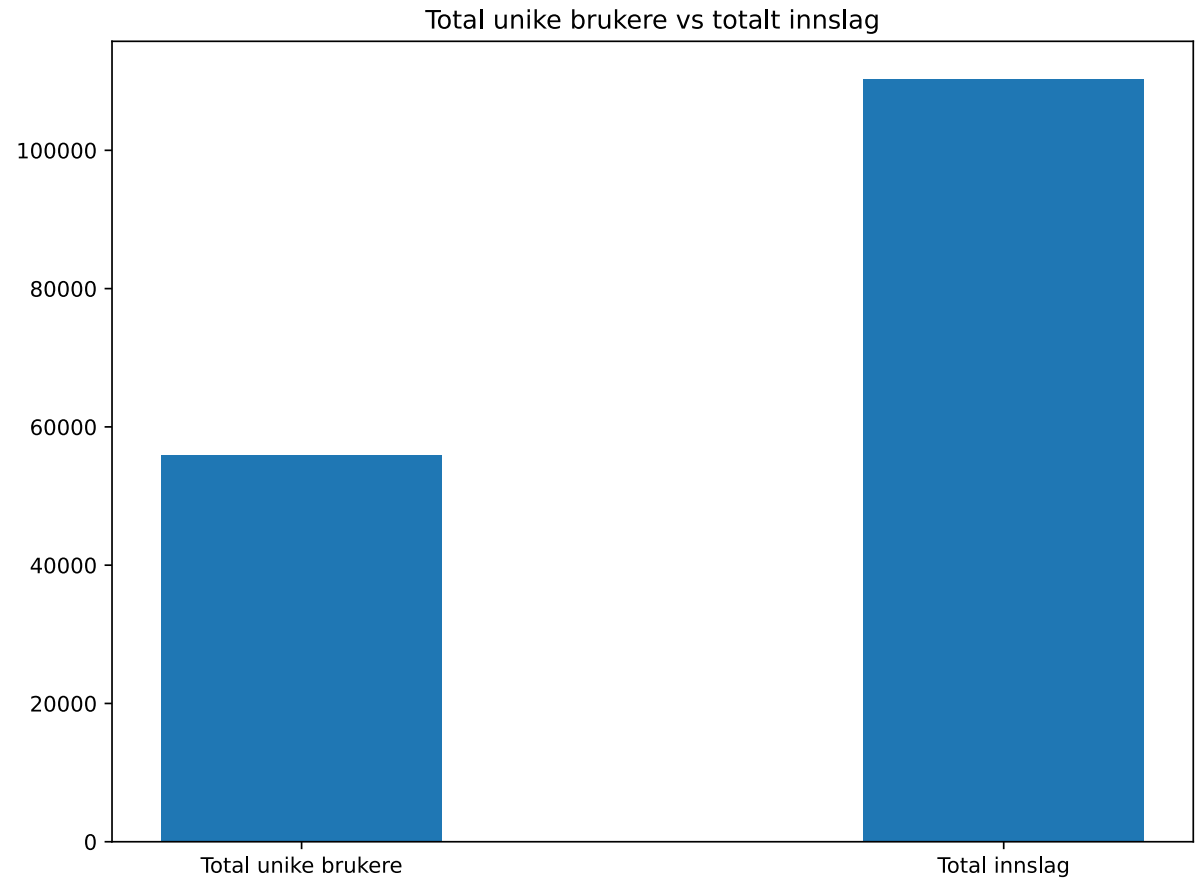


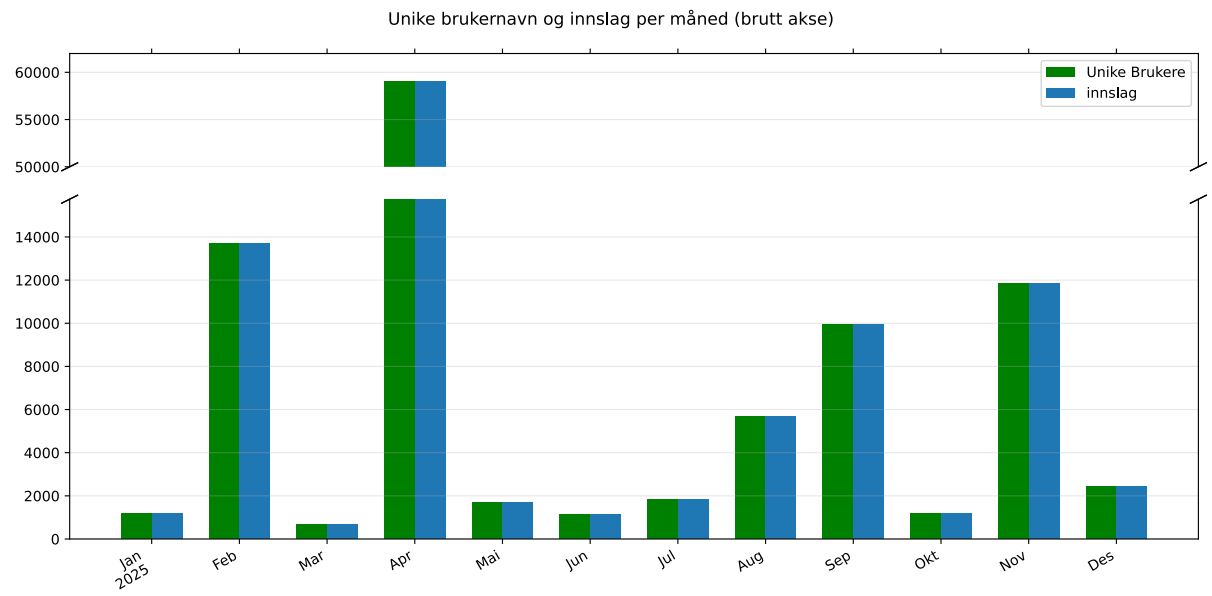
Det foregår til enhver tid mye skanning etter kjente sårbarheter. Noe av dette gjøres av aktører med gode hensikter, skanneren vår er et eksempel på dette. Annet kommer fra angripere, og oppdager de sårbarheter ender det i verste fall med ransomware.

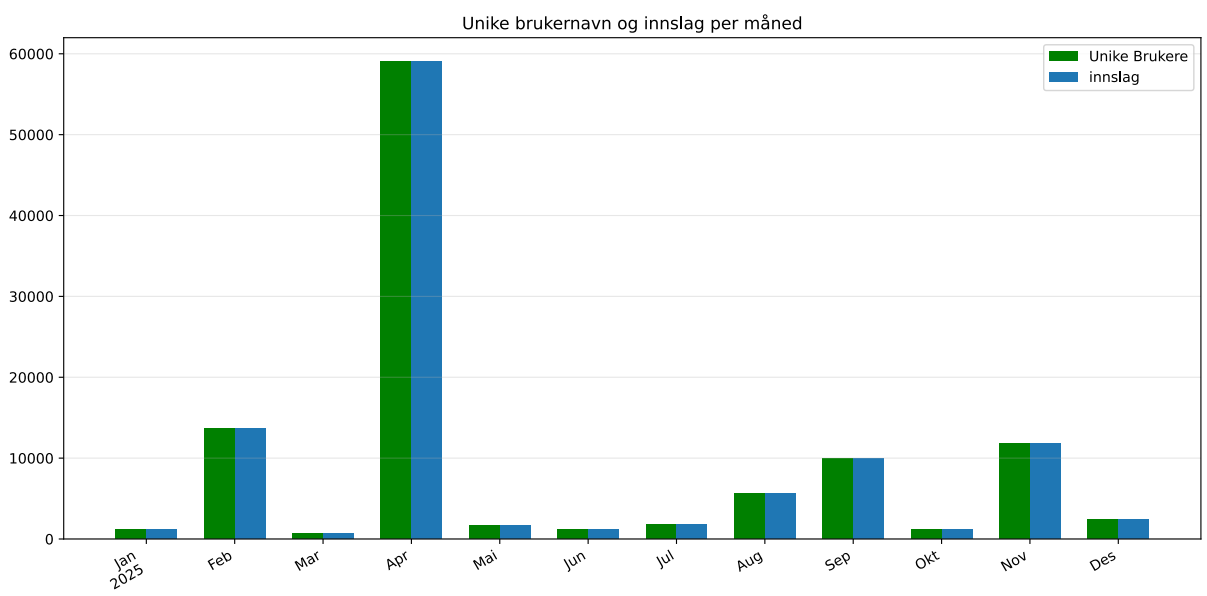
Tiden fra sårbarheter blir kjent til de blir utnyttet er i mange tilfeller svært knapp.

Aggregert NBP 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 «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 2025. Datapunktene er aggregert per måned.

Nevneverdige datasett:

- 2025-02-05: Stealer datasett. Deler av dette datasettet ble sendt ut i sensurert form i 2024.
- 2025-04-02: Historisk datasett. Dette datasettet gikk tilbake til 2023-01-01.
- 2025-09-05: Historisk datasett. Dette datasettet gikk tilbake til 2025-01-01 og er separat fra datasettet hentet i april
- 2025-11-25: Historisk datasett fra Synthient.

Du kan lese mer on tjenesten «Brukernavn og passord på avveie» 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