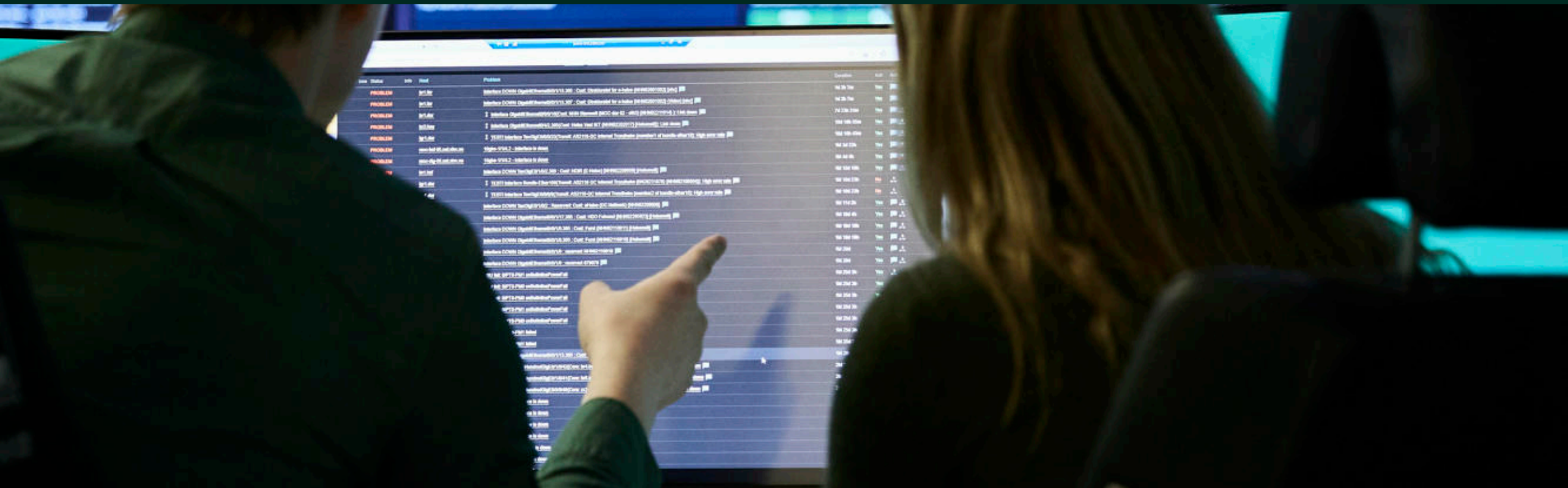
Norsk helsenett

Helse- og KommuneCERT Tilbakeblikk 2. tertial 2025



Nytt fra Helse- og KommuneCERT

Hurtigtest v8.0

Hurtigtest er nå ute i versjon 8, med to nye sjekker og forbedringer på eksisterende.

Av de nye er en sjekk om servere krever signering, noe som forhindrer relay-angrep i nettverket. Dette inkluderer relaying til sertifikatserver (sårbarheten ESC8) som vi ser ofte er mulig hos våre medlemmer.

Videre så vil sjekken «pre2k» avdekke standardpassord på eldre maskinkontoer.

Vi har også forbedret LDAP-sjekken som leter etter usikker konfigurering og tilgjengelige attributter med sensitive personopplysninger.

Hurtigtest versjon 8 ble lansert 12. september. Full endringslogg

Nedlasting

For de av dere som har en Hurtigtest v7 (lansert i februar i år) så vil Hurtigtest sjekke etter ny versjon selv (dere må bekrefte faktisk oppdatering).

Hvis du ikke har lastet ned Hurtigtest før eller har en eldre versjon må du nå logge inn på portal.helsecert.no og laste ned hurtigtest under din medlemgruppe (din virksomhet).
Med denne oppdateringen vil også all framtidig nedlasting gjøres gjennom innlogging i portal. Vi går bort fra nedlasting med nedlastingsID.

For de fleste så vil man bli ledet til rett medlemsgruppe automatisk, gitt at e-posten din er lagret hos oss.
Hvis du bruker en annen e-post enn den vi sitter på, eller ikke er oppført som administrativ eller teknisk kontakt for din virksomhet, så må du be om tilgang til rett medlemsgruppe i medlemsportalen.

Ta kontakt med oss på «post@helsecert.no» ved problemer.

VA-satsing

Vann er kritisk for helse, og er en av de viktigste tjenestene norske kommuner leverer. Dette gjør vann til noe vi vil bidra til å sikre.

På grunn av dette satte vi før sommeren fokus på VA-sikkerhet. Her jobber vi i flere retninger:

1. Det er ofte forskjell på hvem som drifter IT og VA. Vi har gode kontakter på IT, men hadde ikke det for VA. Vi har med deres hjelp begynt å bygge denne oversikten.
2. Vi sender nå ut egne varsel om hendelser som berører vann, både i Norge og internasjonalt. Formålet er å gi dere enkel tilgang til informasjon om hva som skjer i VA-verden på samme måte som vi gjør for IT-hendelser. Si ifra om du vil inn på denne e-postlisten.
3. Vi lager anbefalinger, guider og webinar om VA.
4. Vi har begynt å sikkerhetsteste VA-aktører.
5. Vi leter aktivt etter internett-eksponerte OT, VA og SD-anlegg i Norge. Her har vi gjort hundrevis av funn, for det meste SD-anlegg.

VA	Vann og avløp	-
SD	Sentral driftskontroll	System som f.eks. styrer ventilasjon.
OT	Operasjonell teknologi	Hardware og software som styrer industrimaskiner

Sårbarhetshendelser

Vi operer med to type hendelser. Den første er hvor noen har angriper inne og vi bistår med håndtering av hendelse. Dette er heldigvis relativt sjelden. Den andre typen, som er mye mer vanlig, er sårbarheter som har `potensial for masseutnyttelse`. Vi kaller dette for en sårbarhetshendelse.
Vi sender i snitt ut varsel om kritiske sårbarheter daglig. Fåtallet av disse er sårbarhetshendelser.

Generelt ser vi etter følgende:

- ☐ Sårbarheten gir mulighet til å kjøre kode, eller på annet vis ta kontroll over sårbar enhet.
- ☐ Enheten vil i vanlig oppsett være tilgjengelig på internett.
- ☐ Det er observert angrep **ELLER** angrepskode er tilgjengelig på internett **ELLER** sårbarheten er enkel å utnytte.

Tidsvindu krymper

Vi har de siste årene sett en trend hvor tiden fra en sårbarhet blir kjent, til man ser angrepsforsøk synker. Hvor dette tidsrommet tidligere stort sett var målt i uker og måneder går tiden nå ned mot dager og i noen tilfeller timer. Angrepene kommer raskere, og er ofte del av store kampanjer som systematisk går etter sårbare enheter og forsøker å lage fotfeste på flest mulig av disse. Fotfestet kan senere utnyttes i ro og fred i påfølgende dager, uker, måneder og til og med år.

Det er ikke alle sårbarheter dette skjer med, og hvilke det gjelder er vanskelig å forutse. Treffer sjekklisten over behandler vi det som en potensiell masseutnyttelse.

CVSS er ikke alt

Sårbarheter klassifiseres ut fra et åpent og standarisert rammeverk, «Common vulnerability scoring system» (CVSS) [1] og det benyttes en skala mellom 0 og 10. Høyere score betyr at sårbarheten er mer alvorlig. Samtidig er dette bare halve bildet, noe CVE-2023-38545 [2] i cURL illustrerer bra. Den er scoret med en CVSS på 9,8 (kritisk), samtidig skal det veldig mye til for at den brukes mot deg. For å rammes må du bruke curl med et langt hostnavn mot en Socks5-proxy. Angriper må dermed legge en del forutsetninger til rette, og i tillegg lure offer, dette gjør at vi vurderer sårbarheten som mindre alvorlig enn CVSS alene tilsier. Ser man på listen over har vi kun ett av tre punkter.
I motsatt ende ligger CVE-2025-7775 i Citrix NetScaler [3]. Den har CVSS på 9,2, kritisk, men lavere enn cURL sin. Forskjellen ellers er at Citrix Netscaler er noe man kan forvente å finne direkte tilgjengelig på internett og at sårbarheten her var rapportert som utnyttet når oppdatering kom ut. Den treffer dermed alle punkter på listen vår.

Referanser:

[1] - https://nvd.nist.gov/vuln-metrics/cvss
[2] - https://nvd.nist.gov/vuln/detail/cve-2023-38545
[3] - https://support.citrix.com/external/article/694938

Fra sårbar til OK på … ⏳

Sårbarhetshendelser - En solskinnshistorie

I august hadde Citrix Netscaler (igjen) en kritisk sårbarhet. Sårbarheten traff på alle punkter for å regnes som sårbarhetshendelse for oss. Dere i sektor var responsive og effektive, og sammen lukket vi denne sårbarheten raskt. Under er en gjennomgang som illustrerer hvordan vi jobber i slike sårbarhetshendelser, og hvorfor oppdaterte IP- og domenelister og oppdaterte kontaktpunkter er viktige.

Tidslinje for hendelsen

26.08.25 13:40	Citrix publiserer informasjon om oppdatering for blant annet CVE-2025-7775 [1].
26.08.25 16:29	Vi plukker opp dette og aktiverer vaktfunksjon. Vi vurderer dette som en kritisk hendelse (se vurderingsprinsipper over) og starter arbeidet med å få ut fellesvarsel til medlemmer i NBP.
26.08.25 17:29	Generelt varsel om sårbarhet går ut. Vi søker deretter i skanndata (vi sårbarhetsskanner alle medlemmer kontinuerlig på oppgitte IP-adresser og domener) og finner flere hundre enheter fordelt på 71 virksomheter.
26.08.25 18:12	Vi sender direktevarsel til alle 71 virksomheter, hvor vi i tillegg til å beskrive sårbarheten også lister opp hvilket utstyr som er berørt hos dere.
26.08.25 18:45	Vi ringer samtlige 71 virksomheter med utgangspunkt i (i prioritert rekkefølge): Innmeldt vakttelefon, innmeldte tekniske kontaktpunkter, innmeldte administrative kontaktpunkter, sentralbord på hjemmeside, ansatte på hjemmeside. Der vi ikke får tak i noen sender vi SMS.
26.08.25 21:02	Vi har den tekniske informasjonen vi trenger for versjonssjekk av Citrix NetScaler og dermed finne ut om instanser er sårbare eller ikke.
26.08.25 21:23	Alle 71 virksomheter oppringt, men vi har ikke kommet gjennom hos alle. Vi mangler svar fra 10 virksomheter. Vi fortsetter å forsøke alternative kontaktpunkter.
26.08.25 23:25	Alle bortsett fra fire medlemmer har bekreftet mottak av varsel. De siste fire får vi ikke tak i på telefon eller SMS.
26.08.25 23:35	Automatisk versjonssjekk av alle Citrix NetScalere vi kjenner til satt opp. Det gjenstår nå 61 sårbare NetScalere fordelt på 29 virksomheter.
27.08.25 08:00	40 sårbare NetScalere fordelt på 19 virksomheter.
27.08.25 14:40	Alle medlemmer i NBP har bekreftet mottak av varsel om sårbar NetScaler.
27.08.25 15:10	16 sårbare NetScalere fordelt på 10 virksomheter.
27.08.25 20:40	5 sårbare NetScalere fordelt på 4 virksomheter.
29.08.26 12:52	Siste NetScaler oppdatert.

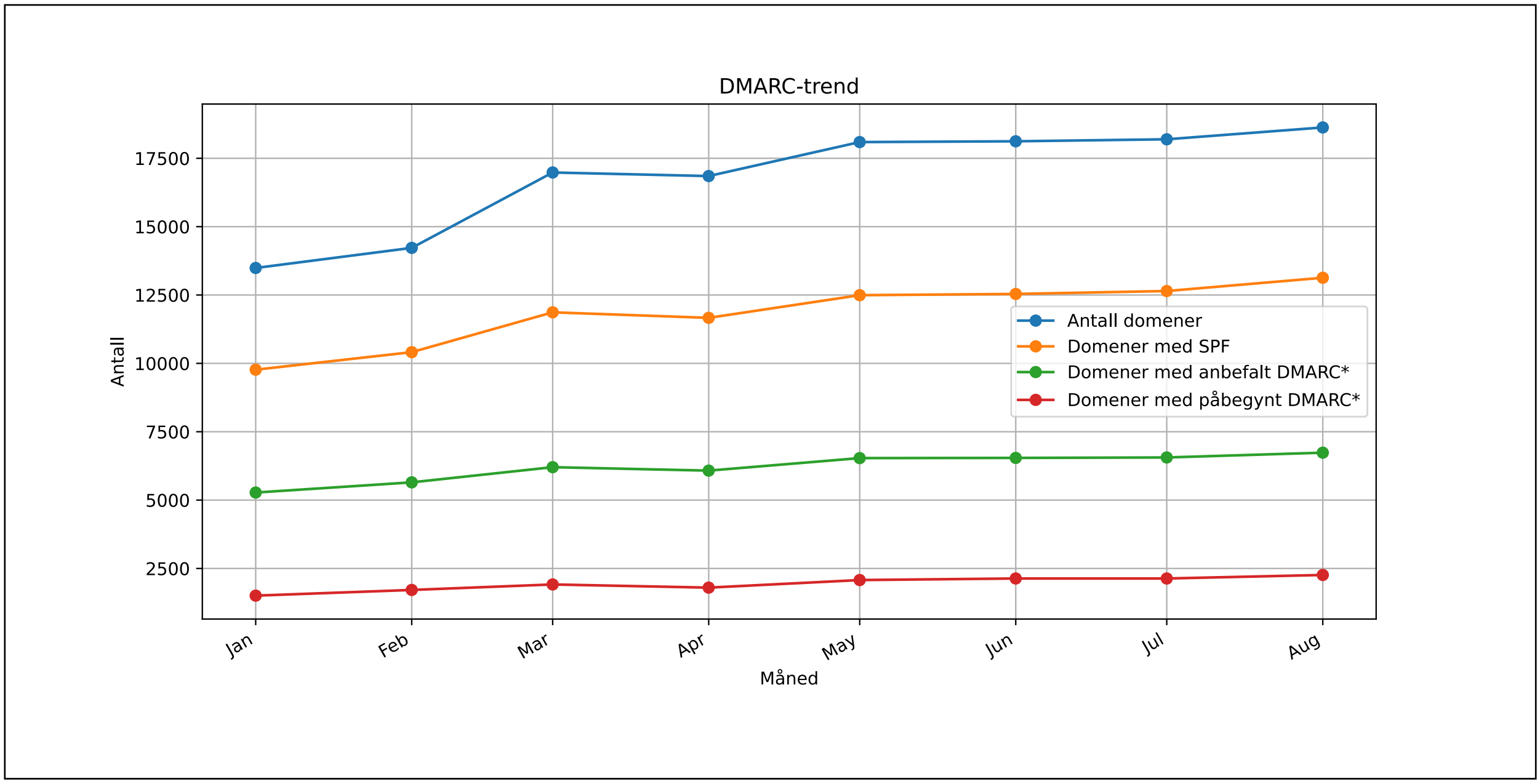
Morsom historie. Hva angår den meg?

- Vi bruker informasjon om domener og IPer for å sikre dere. ← Pass derfor på å holde IP og domenelister oppdatert! Lister er vedlagt tilbakeblikk.
- Innmeldte kontaktpunkter, og spesielt vakt er kjempeviktig for **tidsriktig** varsling ← Pass på at de stemmer
- Her greide vi som sektor å fjerne 90% av slike eksponeringer på godt under 24 timer. Dette er imponerende (og helt nødvendig basert på angrepstrendene). Måltallet her er 100% på under 24 timer. ← Det vil komme flere slike sårbarheter. Forbered dere på det.

* **Ringe**: Når vi ringer om noe etter arbeidstid er det fordi vi mener man burde gjøre noe samme kveld. Både oppdatering, trekke ut strømkabel eller akseptere risiko er løsninger. Vi anbefaler en av de to første løsningene.

[1] - https://support.citrix.com/external/article/694938

DMARC-trend for helse- og kommunesektoren i NBP

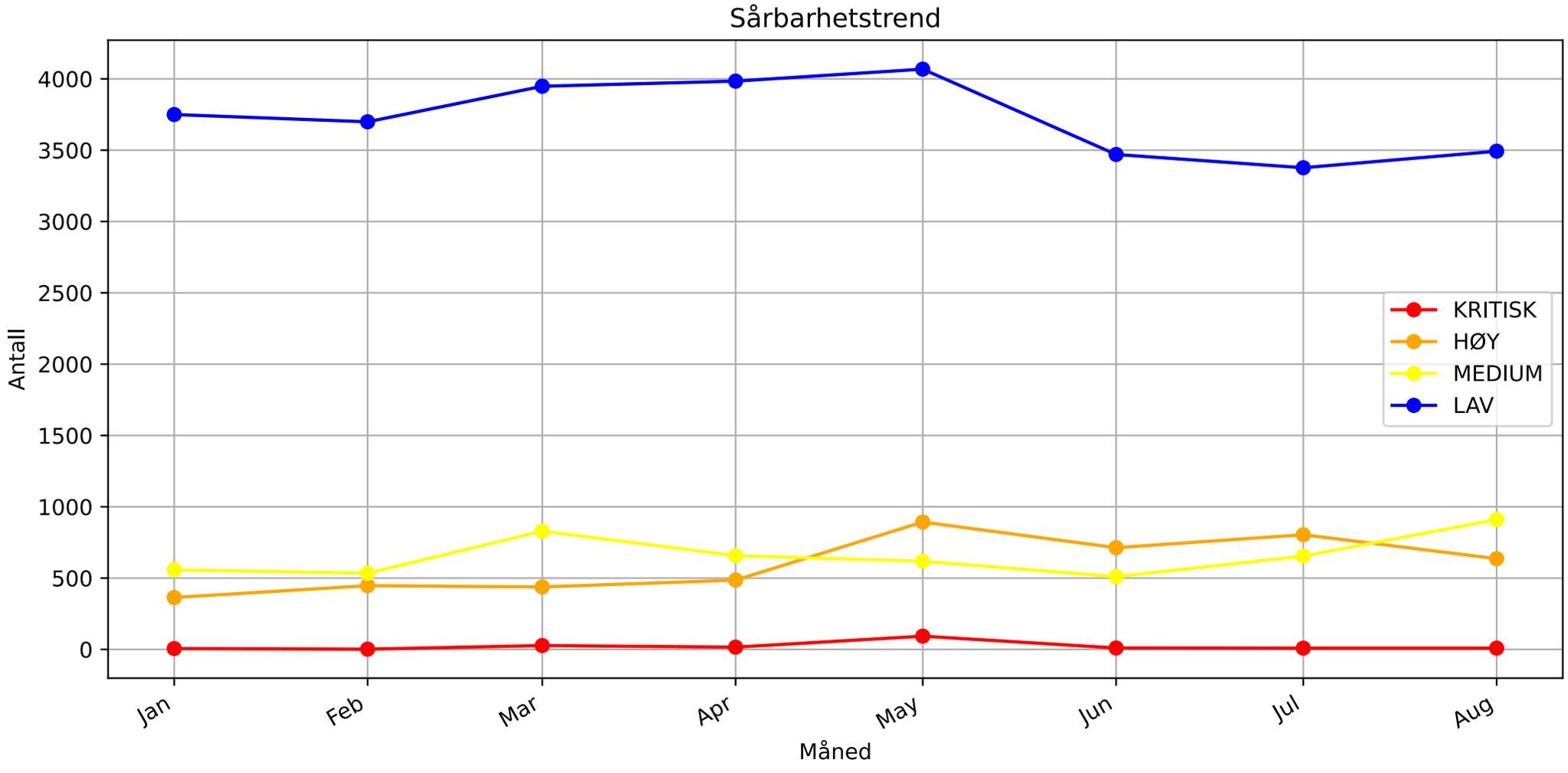


Her er en oversikt over status for DMARC-implementering for hele Nasjonalt beskyttelsesprogram (NBP). Usikrede domener som ikke sender e-post er basert på at domenet ikke har MX-peker og heller ikke har DMARC-record. Unntak kan forekomme, men er sjeldne. For domener som ikke benyttes til å sende e-post, anbefaler vi å sette SPF-record «v=spf1 -all» i TXT-record for domenet, samt DMARC policy p=reject.

*Påbegynt DMARC: DMARC-rapportering er skrudd på, men policy er enten p=none (e-post sendt på vegne av domener som feiler DMARC skal slippes igjennom) eller p=quarantine (ikke definert i DMARC spesifikasjonen hva som skal gjøres). Vi anbefaler policy p=reject (e-post sendt på vegne av domener som feiler DMARC skal avvises). Hvis policy er satt til p=none men rapportering ikke er skrudd på, anser vi ikke at prosessen med DMARC er påbegynt.

*Anbefalt DMARC: DMARC-policy er satt til p=reject.

Sårbarhetstrend for helse- og kommunesektoren i NBP



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