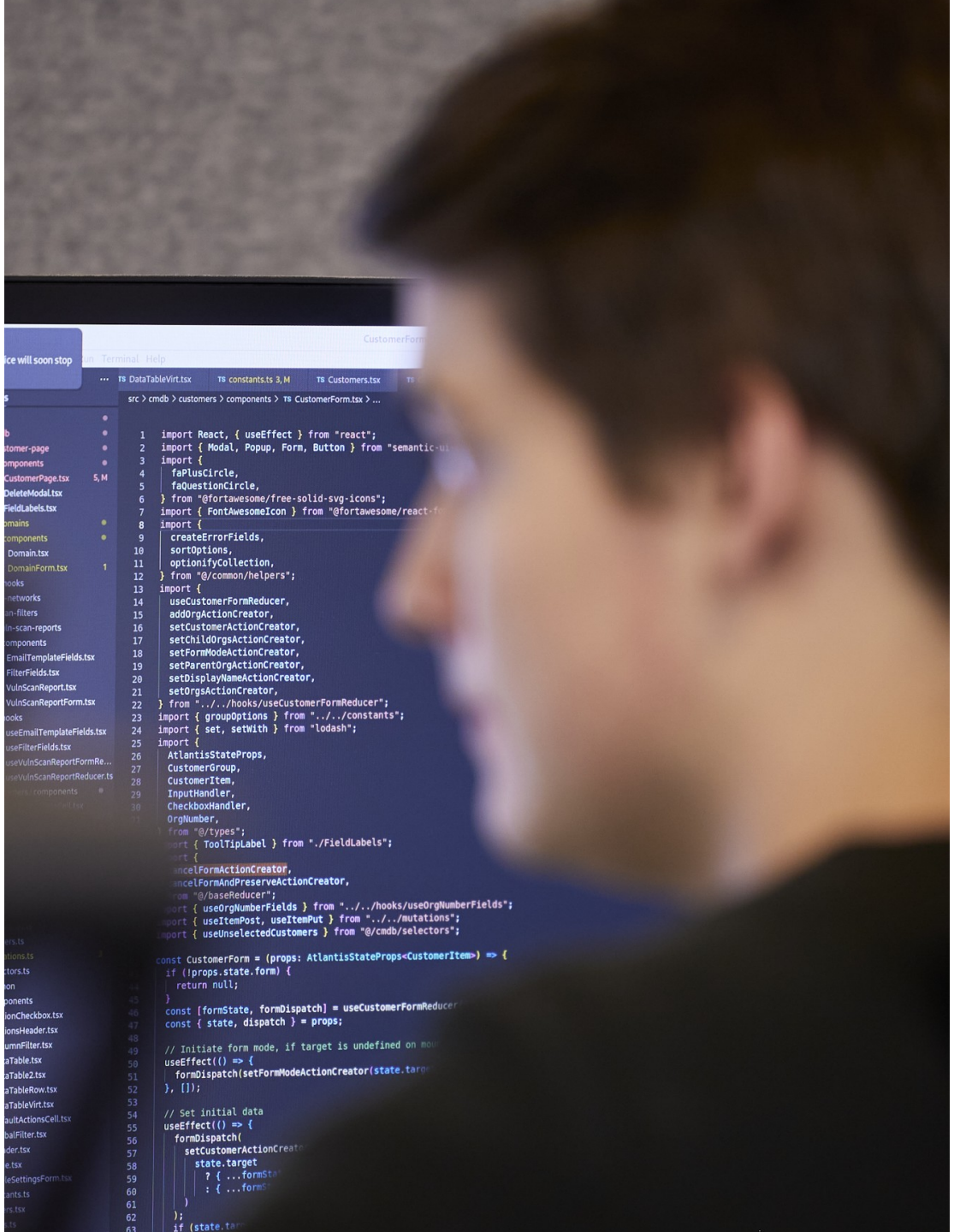
Norsk helsenett

Helse- og KommuneCERT
Tilbakeblikk 3. tertial 2024

Innhold



Nytt fra Helse- og KommuneCERT

Blokkeringslister v3

Grunnet økt bruk og stadig mer aktuelt innhold, har vi valgt å flytte og forbedre vår blokkeringslistetjeneste. Listene inneholder nå tusenvis av adresser som bør blokkeres, og vi anbefaler å flytte til ny løsning så raskt som mulig for ikke å miste beskyttelse. Den eksisterende tjenesten på data.helsecert.no blir skrudd av senest 1. mars 2025.

Hjelpeside med migreringshjelp finnes her:
https://blocklist.helsecert.no/v3
Kun tillatte IP-adresser får tilgang til tjenesten og hjelpesiden. Dersom dere ikke når tjenesten, send IP-adressene dere bruker til post@helsecert.no for hvitelisting.

Windows 10 og Exchange EOL

Microsoft Windows 10 og Exchange vil som hovedregel miste støtte fra 14. oktober 2025. Dette er produkter som spiller en sentral rolle hos flere av våre medlemmer.

I løpet av de siste månedene har vi sendt ut et felles varsel til NBP-info i forbindelse med at Windows 10 mister støtte. I tillegg har vi sendt målrettede varsler til våre medlemmer der vi har identifisert Exchange 2016 eller 2019.

Vi anbefaler at berørte virksomheter planlegger utfasingen av begge produktene i god tid før 14. oktober 2025.

Brukernavn og passord på avveie

Også dette tertialet har vi kommet over mange brukernavn og passord på avveie, og vi jobber for å komplettere denne oversikten. Vi er spesielt bekymret for passord brukt til VPN og annen fjerntilgang.

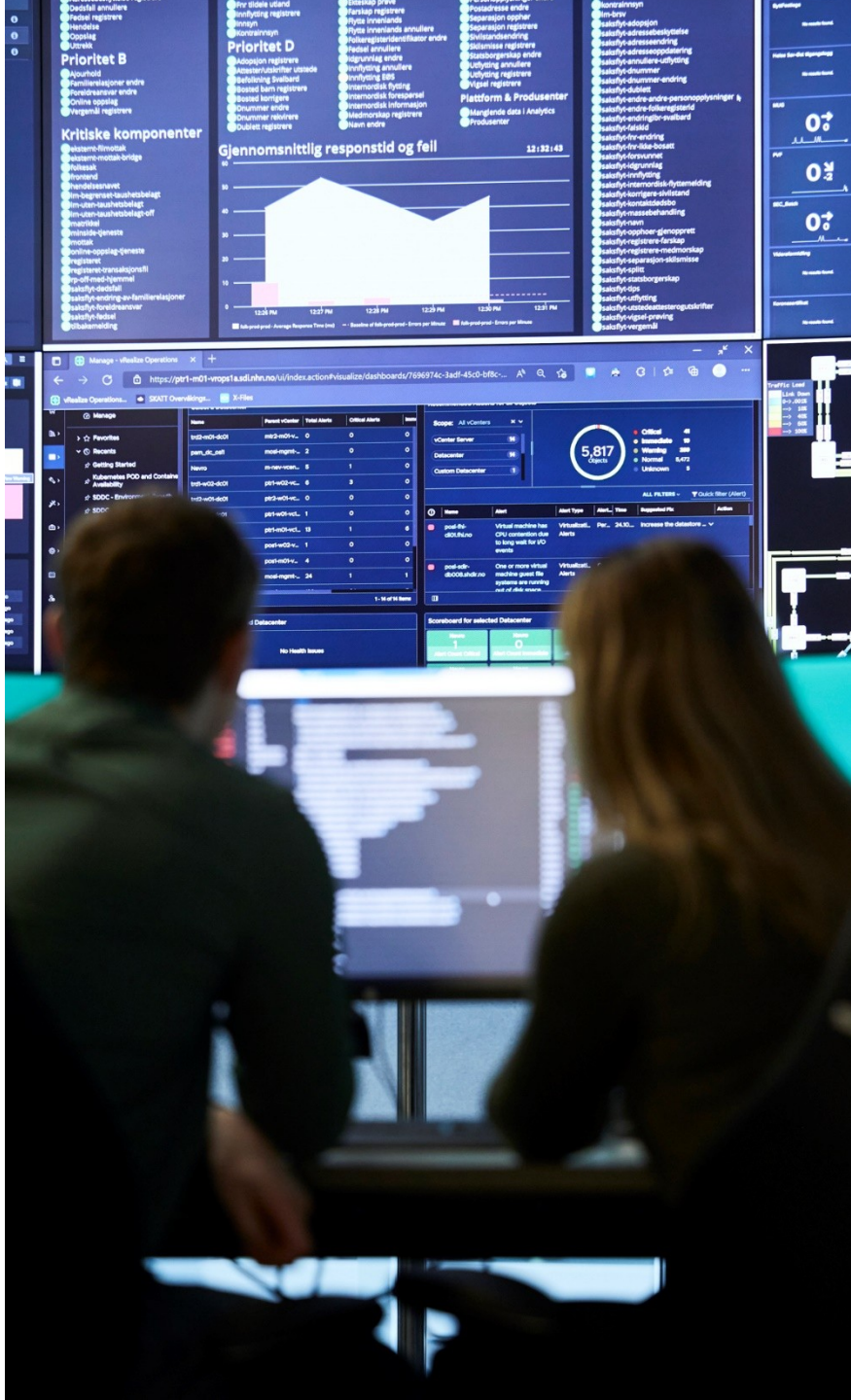
Vi sender nå detaljer usensurert - men kryptert - til oppgitte kontaktpunkter, samt en månedlig oppfølging til hendelseslisten så lenge vi ser ny data for virksomheten.

For å kunne varsle på en god måte trenger vi deres hjelp til å sørge for at oversikten over deres domener er mest mulig komplett! Dette gjelder også tredjepartsdomener som for eksempel: helsecert.onmicrosoft.com

Adminpanel

Vi ser stadig at adminpanel (webgrensesnitt for administrasjon av enheter) er eksponert på internett, og vi ser at disse stadig utnyttes i angrep. Vi merker slike panel som et funn med HØY kritikalitet når vi finner de i skanningen vår.

Disse adminpanelene er, i motsetning til sidene for M365, og tilsvarende skyløsninger, ikke opprinnelig laget for å være eksponert på internett. Dette ser vi reflektert i mengden sårbarheter som oppdages og brukes. Ofte har angrepene også pågått en tid før sårbarheten er kjent for leverandøren selv.



Kommunetest

I november 2024 lanserte vi kommunetest. Testen er tilgjengelig for alle våre medlemmer uavhengig av sektor.
Kravene for å kunne bestille en kommunetest er:
- At dere ikke har nevneverdige funn i sist kjøring av Hurtigtest.
- At dere ikke har alvorlige sårbarheter i sårbarhetsrapporter fra oss.

Gå til Kommunetest for å bestille en test.

Kommunetest er en gjennomgang av de vanligste og mest kritiske sårbarhetene vi gjennom erfaring har sett i helse- og kommunesektoren. Hensikten med en slik test er å øke virksomhetens motstandsdyktighet mot cyberangrep.
Vi har tre utgangspunkt for testen:

1. **Fra internett**
   Med utgangspunkt i Helse- og KommuneCERTs sårbarhetsrapport for virksomheten, ser vi etter sårbarheter i internett-eksponerte tjenester.
   Vi sjekker bruken av multifaktorautentisering (MFA) på tjenester med innlogging fra internett.
2. **Fra klientnett**
   Fra innsiden av virksomheten utfører vi en sårbarhetsskann av alle tjenester vi ser fra innsiden.
   Vi sjekker passordkvalitet av virksomhetens brukere.
   Vi ser etter sensitive data i delte filområder.
   Vi ser etter sårbarheter i Active Directory og andre sentrale systemer.
3. **Fra VDI**
   Vi ser etter sårbarheter i fjerntilgangsløsninger som anvendes av virksomheten.

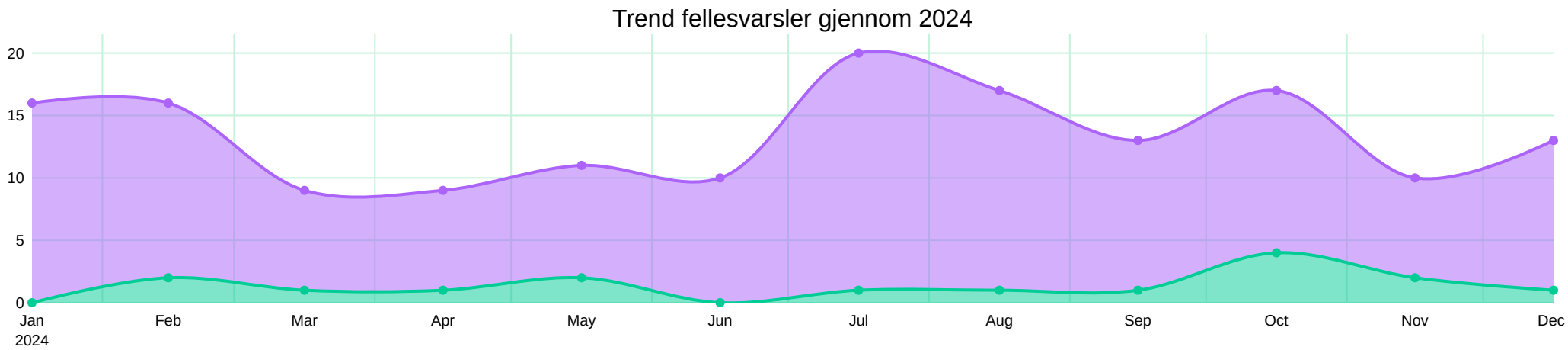
Informasjonsdeling – NBP

Antall fellesvarsler sendt til NBP-saarbarhet-patch gjennom 2024

161

Antall fellesvarsler sendt til NBP-trussel gjennom 2024

16



Tilbakeblikk 3. tertial 2024

Brukernavn og passord på avveie – NBP

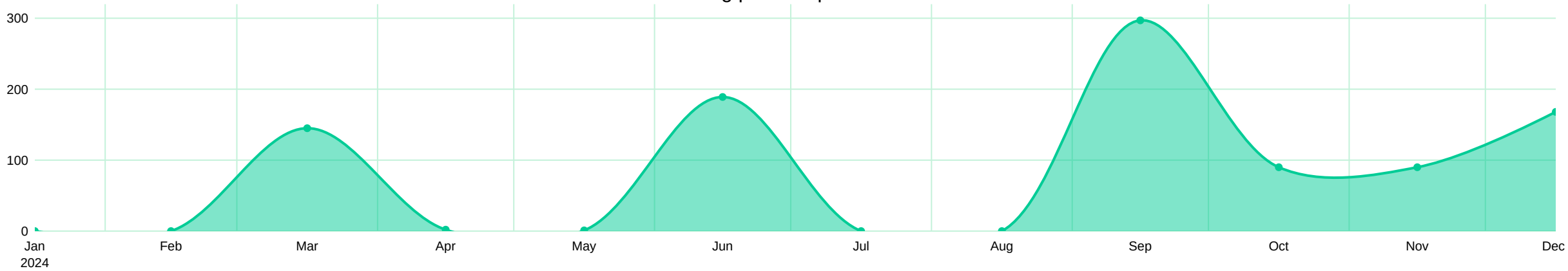
Antall brukere varslet om passord på avveie 2024

8.75k

Antall varsler sendt i 2024

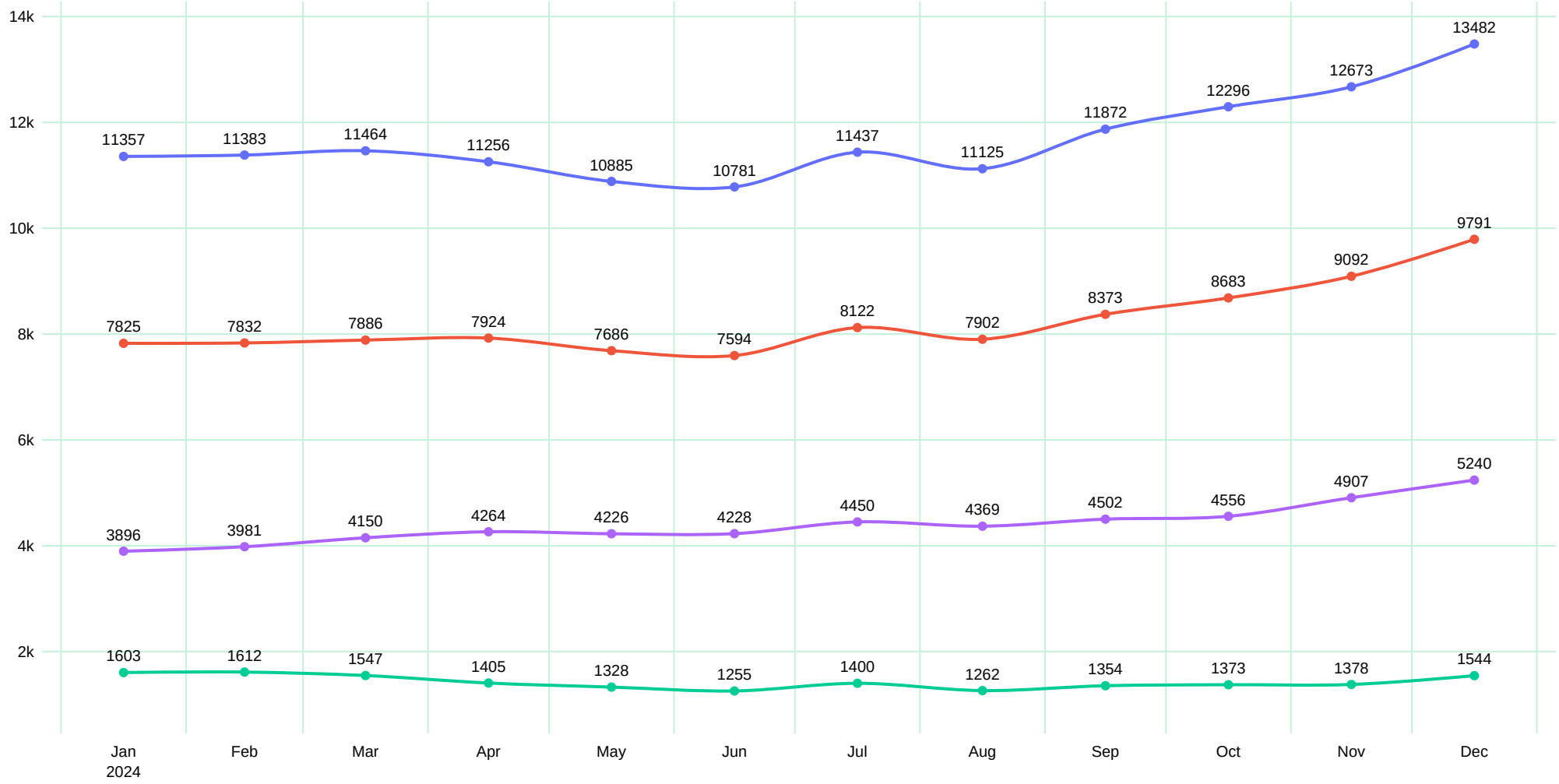
982

Antall varsler om Brukernavn og passord på avveie sendt totalt for NBP i 2024



Beskyttelse mot spoofing - NBP

Spoofing betyr å forfalske avsender. I løpet av siste år har vi registrert flere e-postangrep hvor avsenderadressen har vært forfalsket. Ved å bruke DMARC kan man sikre seg mot at domener blir misbrukt. Som vi ser av grafen nedenfor så er det lav dekningsgrad og få endringer knyttet til DMARC-policy. Vi oppfordrer alle til å bruke egen oversikt for e-postsikkerhet i denne rapporten og følge vår guide for å implementere DMARC. Kontakt oss dersom dere har spørsmål: post@helsecert.no.



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.

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.

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. post@helsecert.no

Gjerne bruk rapporteringsskjema, men det er ikke et krav.

Norsk helsenett

Helse- og KommuneCERT

Tilbakeblikk 3. tertial 2024

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.