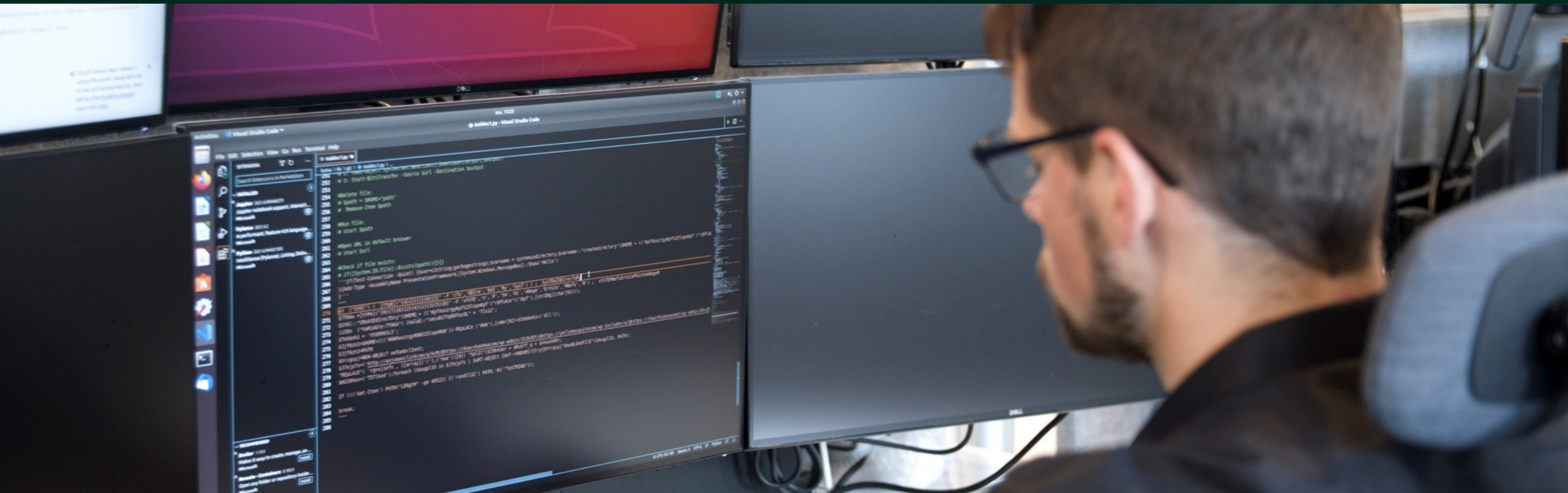
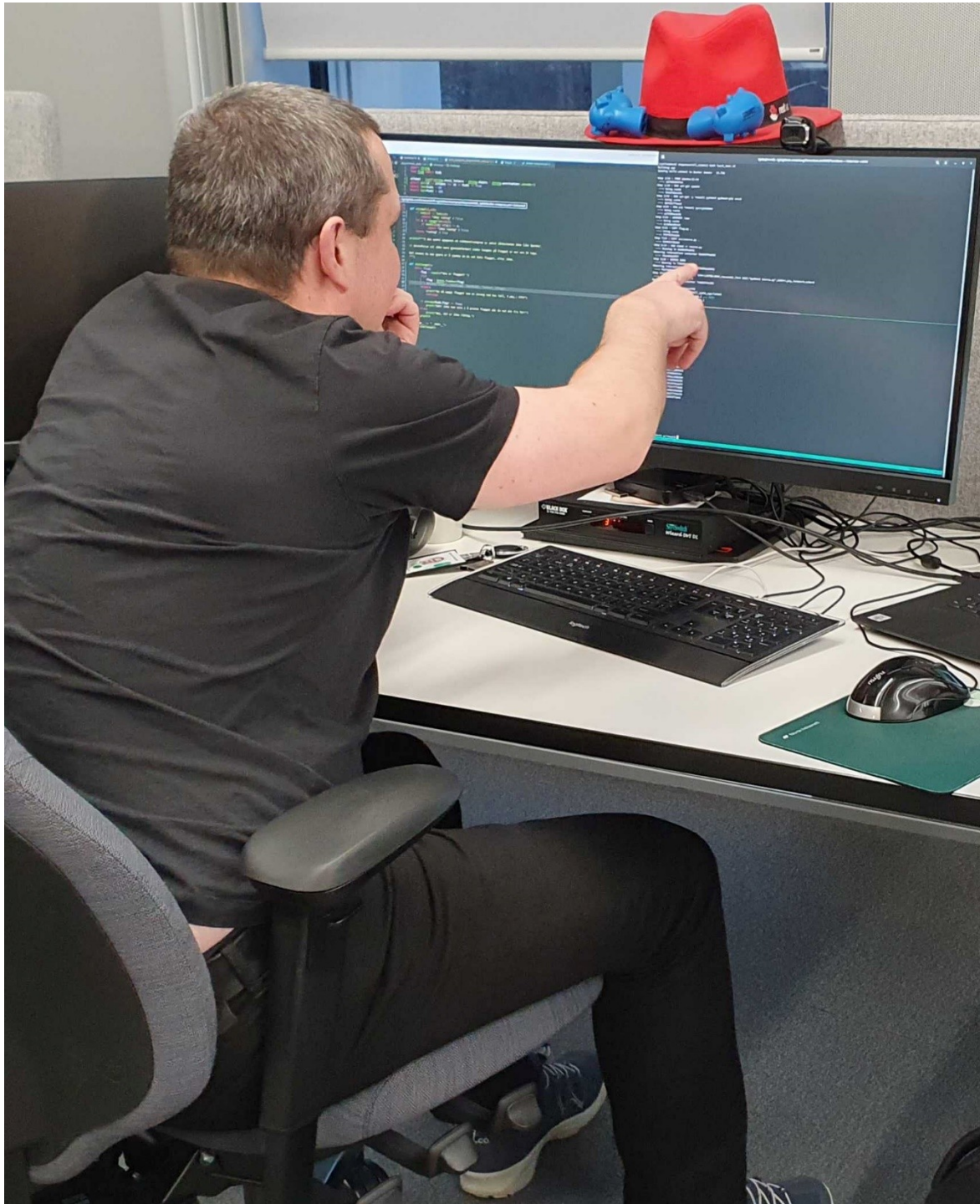
Norsk helsenett

Helse- og KommuneCERT
Tilbakeblikk 2. tertial 2024



Innhold



Nytt fra Helse- og KommuneCERT

AitM-phishing

Vi har brukt mye tid på å følge **A**ttacker-**i**n-**t**he-**M**iddle-phishing (AitM). I et AitM-angrep sitter angriper med automatiserte verktøy som logger inn i sanntid med informasjonen som offer taster inn – inkludert multifaktorautentisering, som effektivt blir omgått.

Flere av dere har fått varsel fra oss om at brukere hos dere er blitt lurt og har fått både passord og sesjonscookie stjålet av angripere. Krav om innrullerte enheter, inkludert sikker innrullering, eller phishingresistent autentisering, vil stoppe slike angrep. Så lenge dette er en trussel mot helse- og kommunesektor vil vi fortsette å jobbe med det.

Kompromittert Wordpress

Siden sist har vi fulgt opp flere kompromitterte WordPress-installasjoner. Dette har tydeliggjort viktigheten av å opprettholde høy sikkerhet for å beskytte nettstedene og brukerne som besøker dem.

Sørg for å bruke den nyeste versjonen av WordPress. Oppdateringer inneholder ofte sikkerhetsfikser som beskytter mot kjente sårbarheter.

Wordpress plugins kan også inneholde sårbarheter. Sørg for at disse holdes oppdatert. Aktiver automatisk oppdatering om det er mulig, og fjern plugins som ikke brukes.

Brukernavn og passord på avveie

Sist tertial har vi kommet over mange brukernavn og passord på avveie. Passordene kommer fra en rekke ulike kilder, som kombolister, skadevare og phishing. Vi går gjennom det som kommer inn, finner ut hvilket domene et passord knyttes til og varsler aktuell virksomhet så raskt vi kan.

Vi er spesielt bekymret for passord brukt til VPN.

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

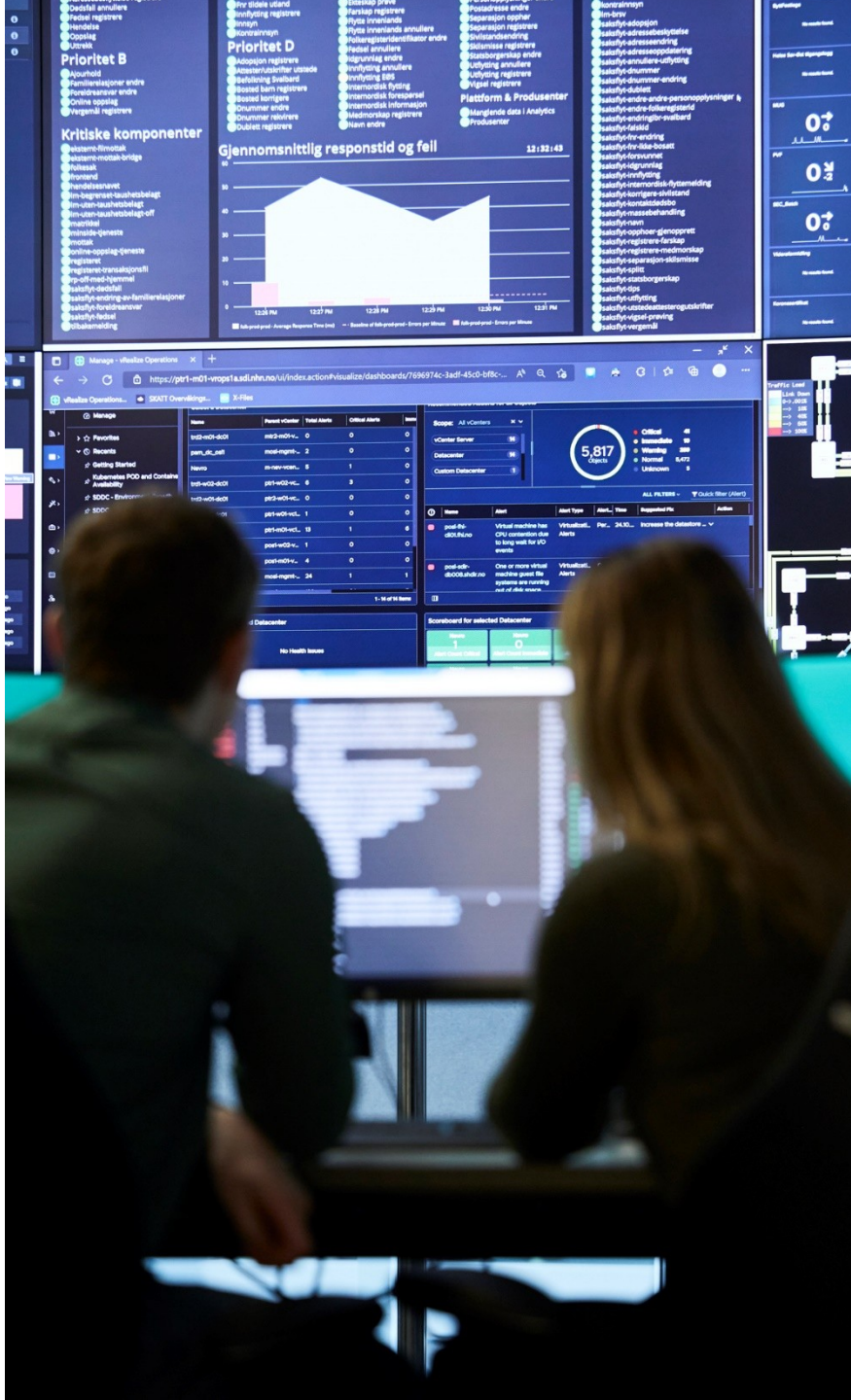
Hurtigtest

Hurtigtest forbedres stadig (Se endringslogg).

Vi anbefaler at å kjøre hurtigtest og utbedrer funnene. Om hurtigtesten er grønn, altså ikke finner noe, anbefaler vi at den kjøres på nytt hvert tertial. Det vil si tre ganger i året.

Dette kan gjerne gjøres i forkant av tertialrapporten/tilbakeblikk, som sendes i januar, mai, september, slik at rapporten har oppdaterte resultater.

Det er uproblematisk å kjøre hurtigtest oftere om man ønsker det.



Varselt(r)etthet

De siste årene er varseltettheten økt. Alle varsel som sendes ut er vurdert ut fra skadepotensial. Faktorer vi vurderer her er **tilgangen** utnyttelse kan gi, **utbredelse** av systemet og hvor sårbarheten kan **utnyttes fra.**

Litt statistikk
I 2020 sendte vi i snitt ut et varsel hver fjerde dag. I 2022 hver tredje. I 2024 nærmer vi oss et varsel annenhver dag.

Varseltetthet øker av flere grunner
Helse- og KommuneCERT er blitt flere, noe som gjør oss i bedre stand til å fange opp, vurdere og sende varsler. Vi har forbedret egne systemer for å fange opp varselverdige sårbarheter. NBP har fått flere medlemmer som spiller oss gode med å si ifra når de savner varsel på noe. Sist, men ikke minst: Antall rapporterte sårbarheter øker.

Varseltretthet
Vi er veldig bevisst på at vi må unngå varseltretthet og en ulv-ulv-effekt. Vi vurderer, som nevnt over, alle sårbarheter ut fra skadepotensial og antatt eller observert utbredelse av systemet i helse- og kommunesektoren. Hver uke er det flere alvorlige sårbarheter vi etter en vurdering ender med å ikke varsle på.

Direktevarsler i stedet for alt som fellesvarsel?
Vi har vurdert å sende kun direktevarsler, men har ikke innsikt nok i våre medlemmers infrastruktur til å være sikre på at vi når ut til alle som bruker programvaren vi varsler om. Det har skjedd at vi kun har sendt direktevarsler, med den konsekvens at sårbare systemer ikke ble fanget opp. Dette vil vi unngå i fremtiden. Vi kommer til å fortsette med direktevarsler, men som et tillegg til fellesvarsler. Formålet med direktevarsler er å understreke viktigheten av å utbedre en sårbarhet, samt at vi har mulighet til å følge opp virksomheten direkte.

Hva kan dere gjøre?
Vi skriver varslene våre for at tittel og oppsummering skal gjøre det tydelig hva de handler om. Følgende kan man sortere varselet i kategorien "*dette har vi, jeg må se på resten av varselet*" eller "*dette har vi ikke, aktiver søppelkurv*". Om dere ikke har full kontroll på om dere bruker et system, anbefaler vi at dere sjekker. Dette gjør det også mulig å opprette innboksregler som sorterer ut irrelevante varsler.

Med hilsen
Helse- og KommuneCERT
- sammen gjør vi Norge sikrere!

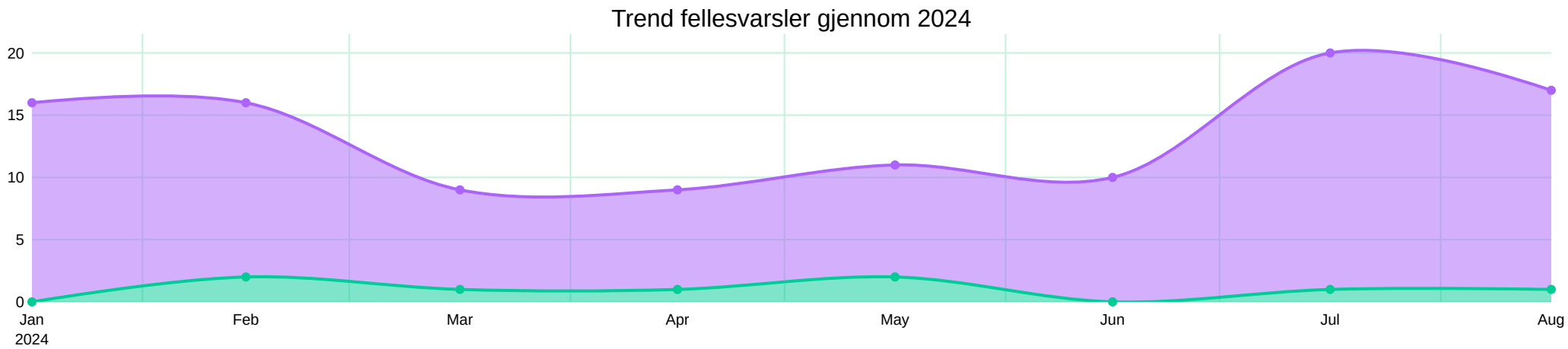
Informasjonsdeling – NBP

Antall fellesvarsler sendt til NBP-saarbarhet-patch gjennom 2024

108

Antall fellesvarsler sendt til NBP-trussel gjennom 2024

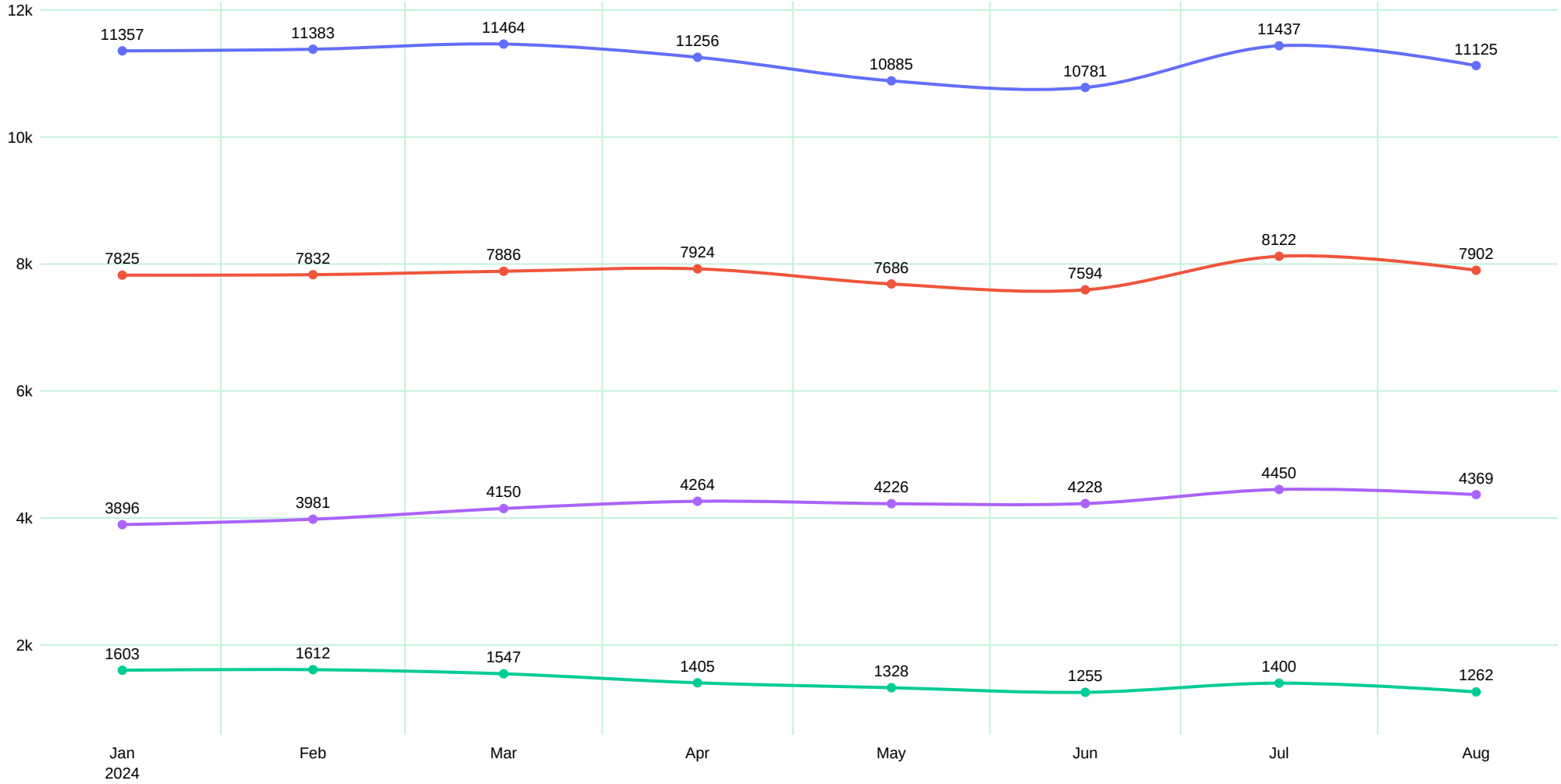
8



Tilbakeblikk 2. tertial 2024

Beskyttelse mot spoofing - NBP

Spoofing betyr å forfalske avsender. Vi har i løpet av siste tertial registrert flere e-postangrep hvor e-postadressen har vært forfalsket. Ved å ta i bruk DMARC kan man sikre seg mot at domener blir misbrukt. Som vi ser av grafen nedenfor så er det lav dekningrad og lite 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.

Tilbakeblikk 2. tertial 2024

Anatomy of an AitM phish; Hvordan gjør de det?

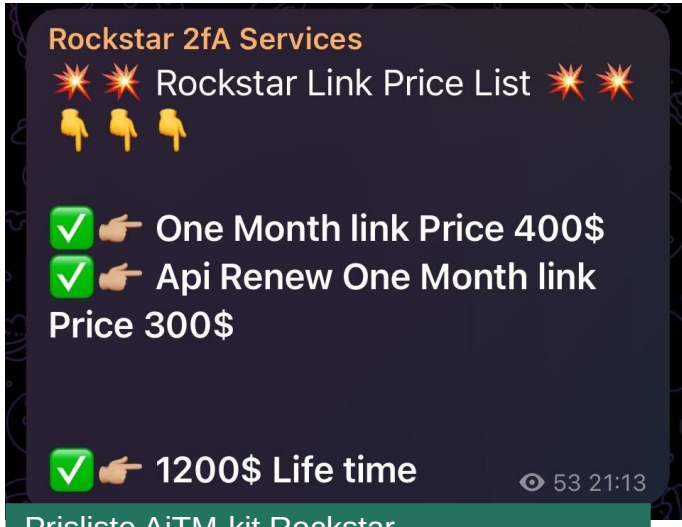
- Siden multifaktorautentisering (MFA) har blitt mye mer utbredt og krever nye teknikker for å omgås, har det oppstått et marked for kjøp og salg av verktøy for dette. Dette kalles AitM phishing.
- For tiden sporer vi mellom fem og ti ulike verktøy eller tjenester for AitM phishing.
- Noen slike verktøy er gratis og må settes opp selv, som det finnes gode guider for. Andre koster mellom 1000 og 5000 kroner i måneden og kommer enten med grundig veiledning eller som en ferdig tjeneste som man kan abonnere på.
- Dette betyr at angriper slett ikke trenger å være spesielt teknisk dyktig for å lykkes med å bryte seg inn i kontoer som er sikret med MFA. En god presentasjon rundt konseptet AitM finnes her.

Måten det teknisk fungerer på er:
1. Offeret logger på phishingkittets falske innloggingssside, som bruker de samme innloggingsdetaljene til å logge på Microsoft Entra ID i bakgrunnen. Dette vil sende en MFA-forespørsel til offerets mobiltelefon. Hvis det kreves nummermatching, vil phishingkittet hente inn disse numrene og vise dem til offeret som da skriver dem inn på mobiltelefonen.

2. Phishingkittet bruker deretter innloggingsdetaljene til å logge inn med nettleser fra en ikke-innrullert enhet. Metoden er lik enten SMS eller Authenticator brukes til MFA. Resultatet er at phishingkittet mottar en gyldig sesjon-cookie som oversendes til angriper sammen med brukernavn, passord og stedsinformasjon.

3. Ved å injisere sesjon-cookien i sin egen nettleser, vil angriperen automatisk være innlogget så lenge cookien er gyldig. I dette steget ser vi ofte at angriper logger på en proxy eller VPN som gir norsk IP-adresse for å virke mindre mistenkelig. Vi har også sett angripere bruke egne virtuelle servere i Norge for å jobbe mot Entra ID.

Som regel vil phishingkittet hente ut sesjon-cookie fra andre land enn Norge. Vi har imidlertid også sett enkelte tilfeller av at dette gjøres fra eller via norske IP-adresser. Vi forventer å se mer bruk av norske IP-adresser framover. Geoblokkering som krever innlogging fra norske adresser er derfor et tiltak som vil få mindre effekt i fremtiden. Per i dag kan det likevel redusere risiko.



Prisliste AiTM-kit Rockstar

Prisliste AiTM-kit Tycoon

Anbefaling – phishingresistent 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), Windows Hello med mer.

Vi anbefaler å kreve

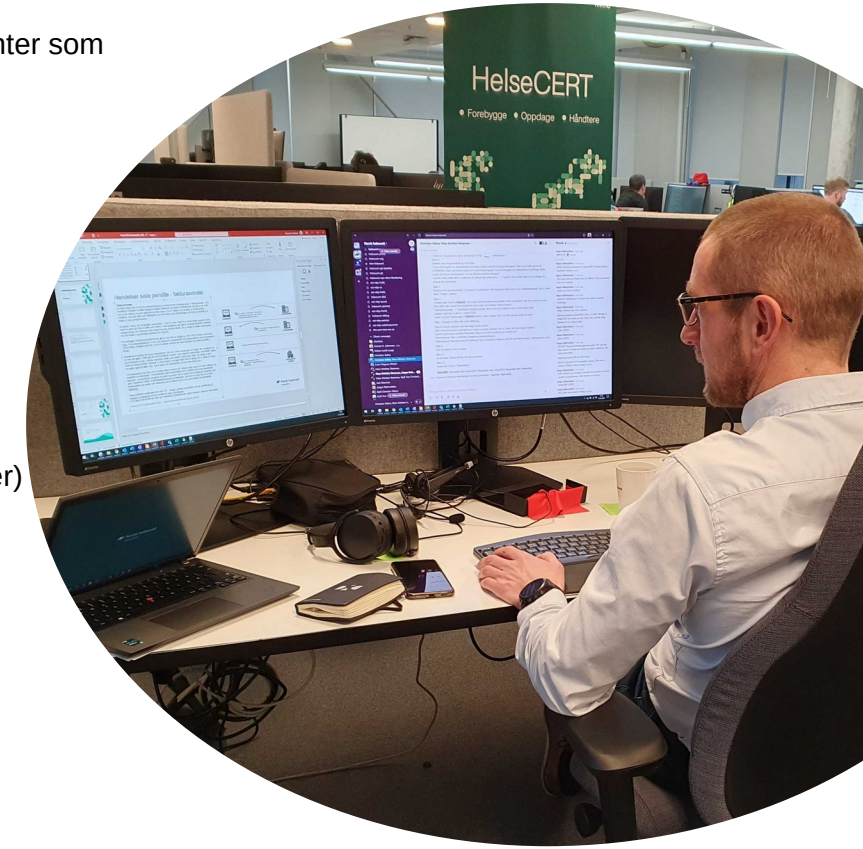
- Innrullert enhet

- Innrullert enhet/Compliant device vil si en enhet som er administrert av virksomhet, 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). Se punkt under.

ELLER

- Passnøkler

- Hvis man **ikke** kan kreve innrullert enhet for innlogging, eksempelvis på grunn av BYOD eller bruk av innleide konsulenter som allerede har enheten innrullert andre steder, bør passnøkler avkreves.
    - Det faller inn under det Microsoft definerer som phishingresistent autentisering
    - Dette kan gjøres både i programvare og maskinvare
    - Dette gir en vesentlig bedre brukeropplevelse enn ordinær multifaktorautentisering



Hva annet kan gjøres?

- Hvis man av ulike årsaker ikke kan kreve innrullerte enheter eller passnøkler, er det fortsatt tiltak som gjennomføres for å redusere risiko. Merk at disse tiltakene ikke er fullgode, men kan redusere risiko betraktelig sammenlignet med å ikke ha dem.
  Dette kan være særlig aktuelt for sikring av elev-kontoer:
    - Begrens mulighet for innlogging fra ikke-innrullerte enheter til kun norske adresser (lokasjonsbasert/geo block)
    - Bruk våre blokkeringslister i conditional access (IP-adressebasert – NB! Merk at det også ligger hele IP-nett her)
    - Benytt risky users / risky sign-ins. 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.

- **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

Norsk helsenett

Helse- og KommuneCERT

Tilbakeblikk 2. 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.