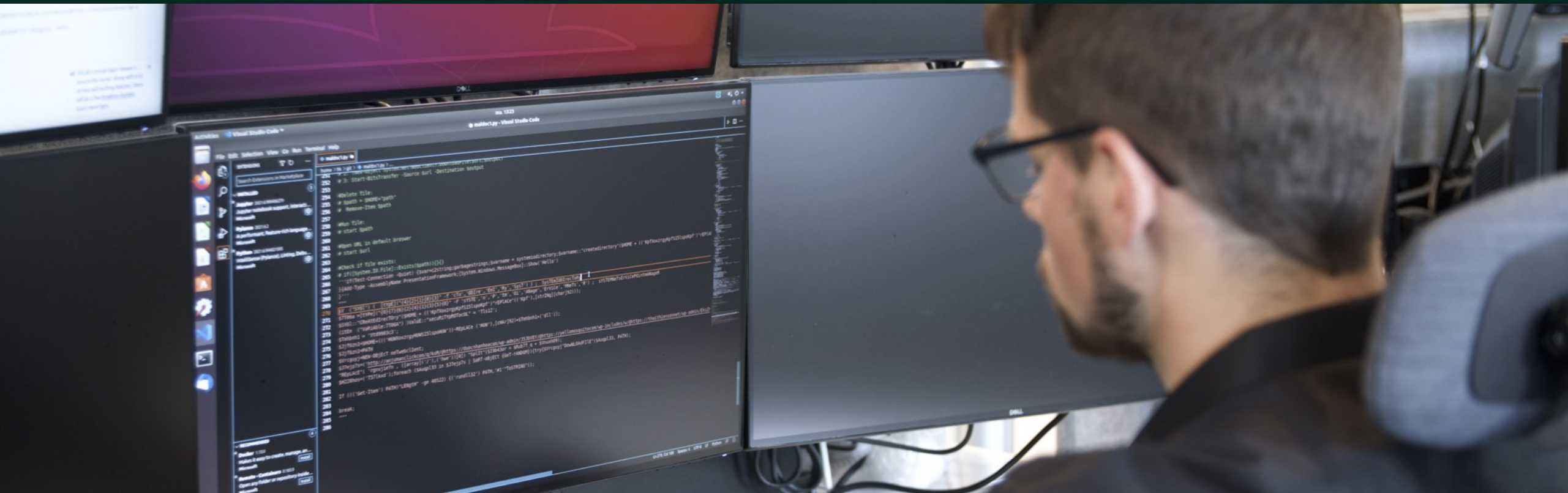
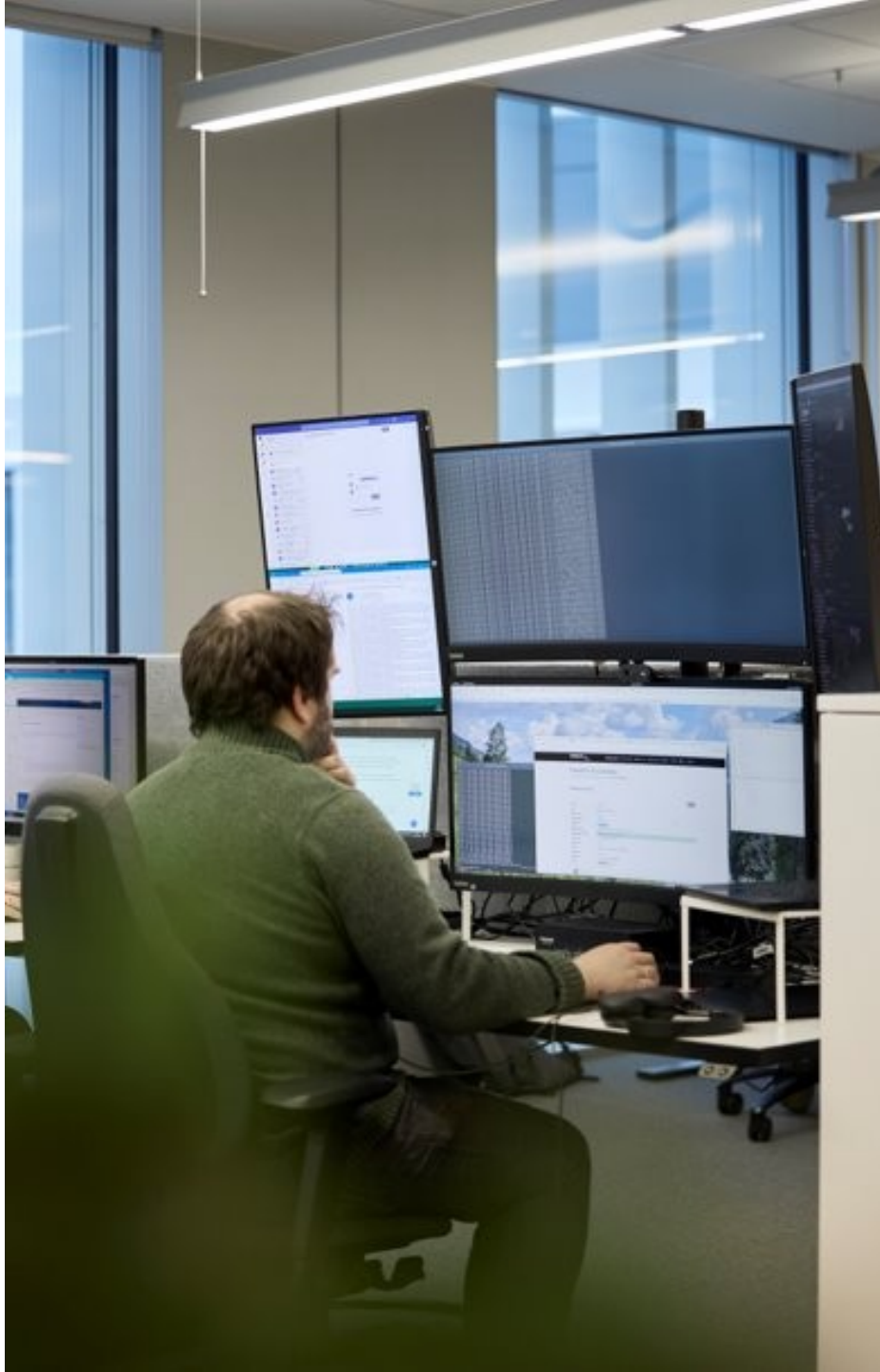
Norsk helsenett

Helse- og KommuneCERT
Tilbakeblikk 1. tertial 2024



Innhold



Være beredt til å håndtere hendelser og sårbarheter - kanskje viktigere enn noen gang!

Det meste av hendelser vi har jobbet med siste tertial har vært knyttet til oppfølging av alvorlige sårbarheter i internetteksponerte tjenester. Det har gjennom det siste året blitt avdekket en rekke alvorlige sårbarheter i systemer som er ment for å være eksponert på internett, som VPN-mottak. Disse sårbarhetene har ofte først blitt utnyttet i målrettede operasjoner av statlige aktører, men senere – og ofte raskt etter publisering – blitt utnyttet til massekompromitteringer. Viktigheten av å håndtere slike sårbarheter raskt er blitt viktigere og viktigere.

Vi har gjennom vårt månedsfokus, så langt i år valgt å sette fokus på tre ulike tema:

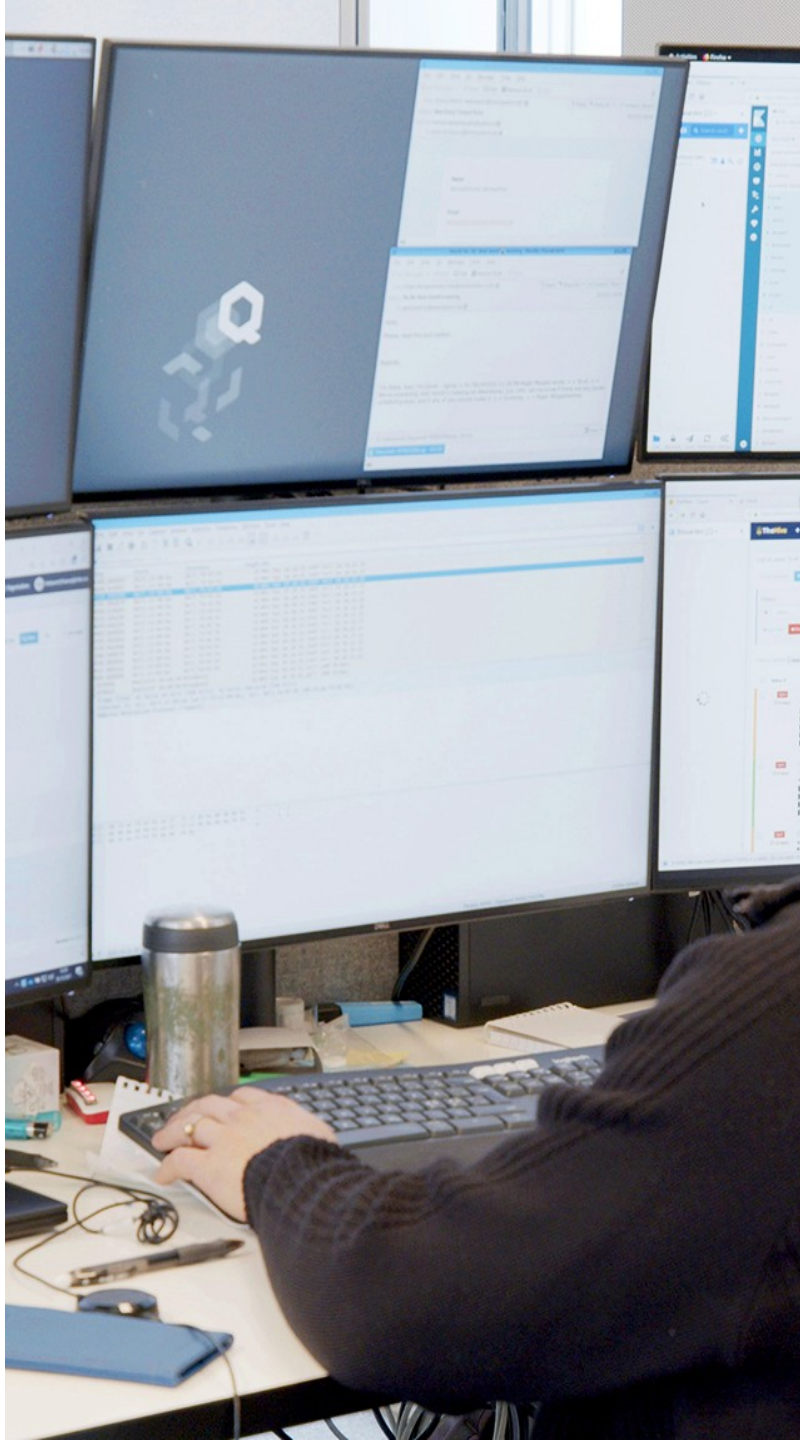
- Hurtigtest
- Redusere angrepsflate
- Herding av MS Entra ID

Alle temaene har blitt fulgt opp med informasjon, webinarer og workshops. Vi har fått bra tilbakemelding og vi ser at mange av dere har lagt ned en god jobb i å følge opp våre anbefalinger. Vi oppfordrer alle til å fortsette å jobbe med disse temaene.

«Nasjonal sikkerhet er et felles ansvar». Det er undertittelen på rapporten Risiko 2024 fra Nasjonal sikkerhetsmyndighet (NSM). Det peker på at når statlige trusselaktører kartlegger verdier og utnytter sårbarheter så er det ikke nødvendigvis topp-politikere, store industrikonsern eller Forsvaret som er inngangsporten. Det kan like gjerne være en leverandør, en kommune, sykehus eller andre virksomheter som angripes, enten fordi de er det direkte målet eller at de brukes for å få tilgang til det egentlige målet. Derfor er det viktig at vi alle tar cybersikkerheten på alvor. God sikkerhet handler i stor grad om god og sikker drift. Det innebærer å ha oversikt over alle systemer, fjerne programvare og tjenester som ikke brukes, ha gode rutiner for oppdatering og herding, god tilgangsstyring, ha kontroll på brannmurregler, m.m. Vårt beste og viktigste forsvar starter med å ha disse grunnleggende tingene på plass.

På de neste sidene vil dere finne flere anbefalinger og konkrete råd fra oss i Helse- og KommuneCERT.

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



Nytt fra Helse- og KommuneCERT

Ny versjon av portskannrapporten

I forbindelse med månedens tema for februar – reduser angrepsflate – gjorde vi en rekke forbedringer i portskannrapporten vår. Rapporten gir en oversikt over deres angrepsflate på internett.

Vi anbefaler at dere bruker rapporten for å lukke/avvikle porter som ikke trenger å være åpne på Internett.

Ved å minimere angrepsflaten på Internett til kun høyst nødvendig tjenester vil dere redusere risikoen for å bli rammet av datainnbrudd.

Nasjonalt beskyttelsesprogram

Gjennom nasjonalt beskyttelsesprogram for helse og kommunesektoren tilbyr vi en rekke tjenester for virksomheter i sektoren. Formålet med tjenestene er å bidra til å heve sikkerheten i sektoren.

For en komplett oversikt over hvilke tjenester vil tilbyr og hvordan dere tar de i bruk, se helsecert.no.

KommuneCERT

Norsk helsenett og HelseCERT fikk i november oppdrag om å etablere KommuneCERT.
Helse- og KommuneCERT er nå fullt operativt som sektorvis responsmijø både for helsesektoren og kommunesektoren. Vi er ett og samme miljø som nå jobber både mot kommune- og helsesektoren. Alle kommuner og fylkeskommuner får nå tilgang til alle tjenester vi tilbyr.

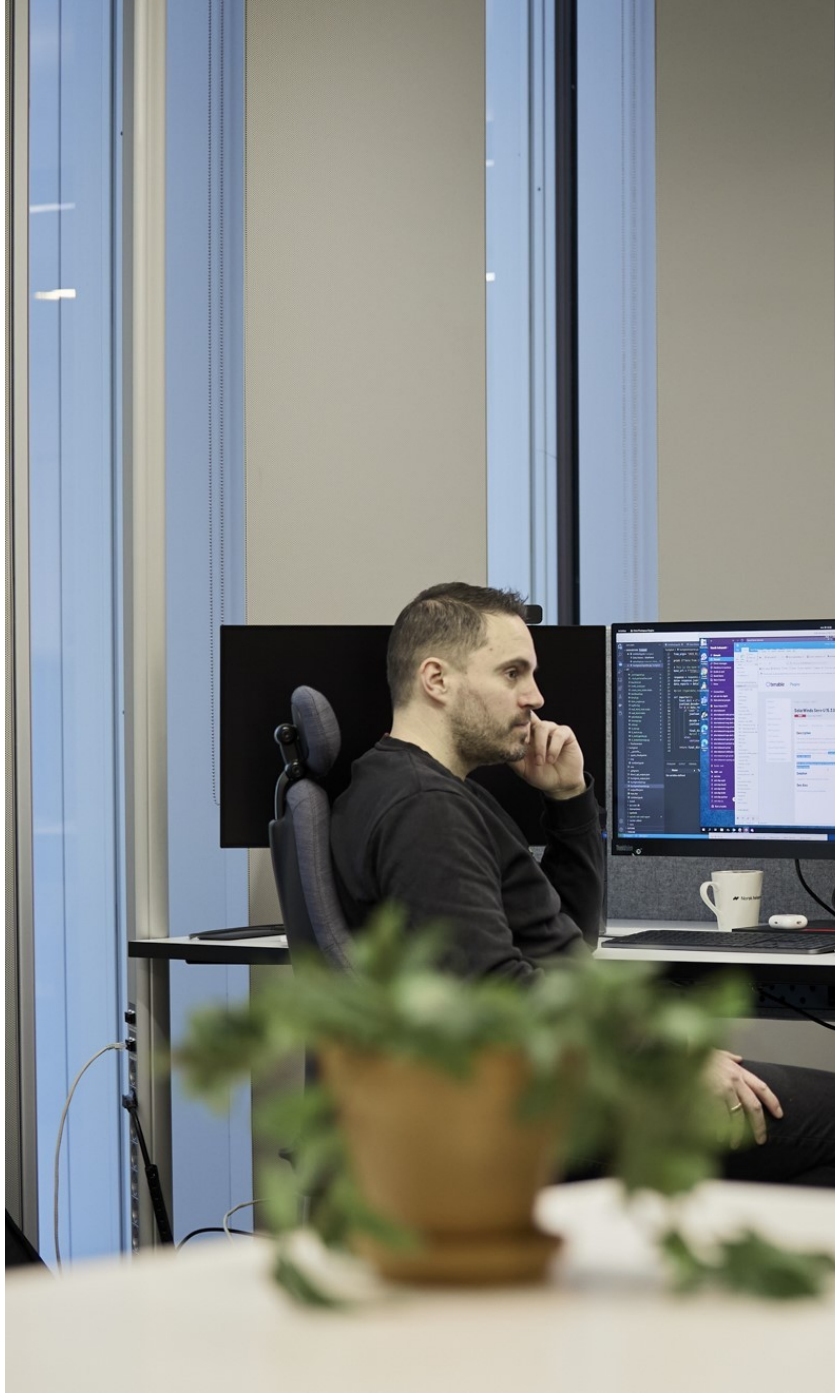
Vår kontaktinformasjon:
E-post: post@helsecert.no
Telefon: 24 20 00 00 – spør etter Helse- og KommuneCERT. Tilgjengelig 24/7 for akutte hendelser.

Webinarer

Vi kjører regelmessig webinarer innenfor ulike tema.

Opptak av alle webinarer ligger tilgjengelig på våre nettsider. Der finner dere webinarer om hvordan dere kan herde deres Microsoft Entra ID, redusere angrepsflate og informasjon om hendelser vi har jobbet med.

Kom gjerne med forslag til tema dere ønsker å høre mer om. Send oss en e-post til post@helsecert.no.



Informasjonsdeling – NBP

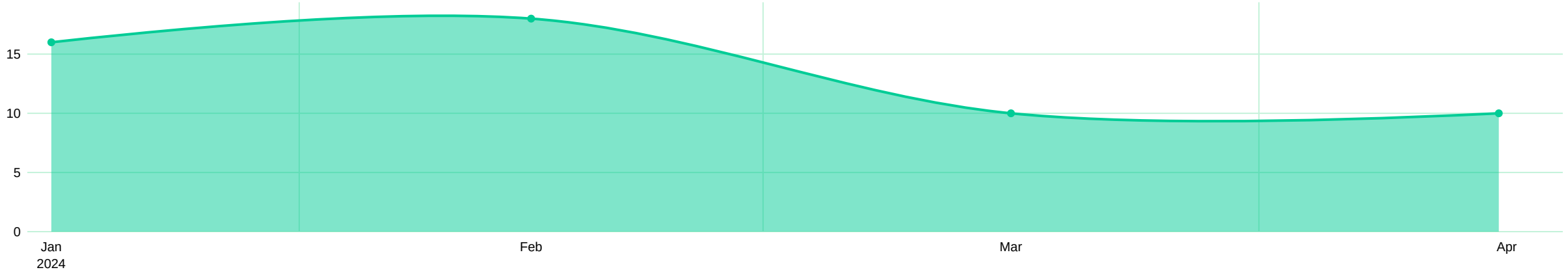
Antall varsler sendt til NBP-saarbarhet-patch siste tertial

50

Antall varsler sendt til NBP-trussel siste tertial

4

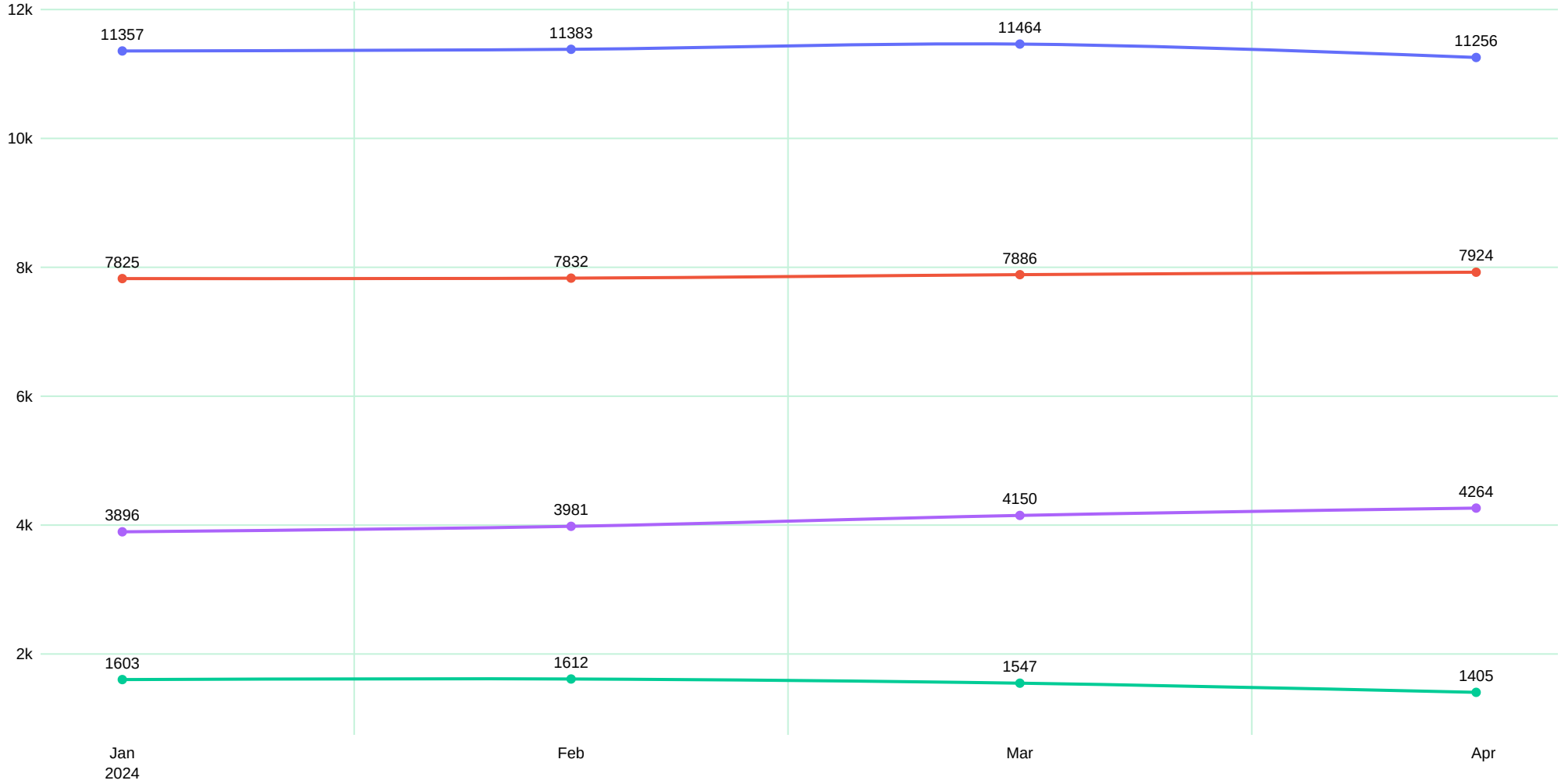
Trend antall varsler siste tertial år



Tilbakeblikk 1. tertial 2024

Beskyttelse mot spoofing

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 kun 38% av de 11256 domene vi kartlegger som bruker anbefalt 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.

Hendelser siste tertial

Phishing
Vi ser hovedsakelig tre ulike typer phishingangrep:

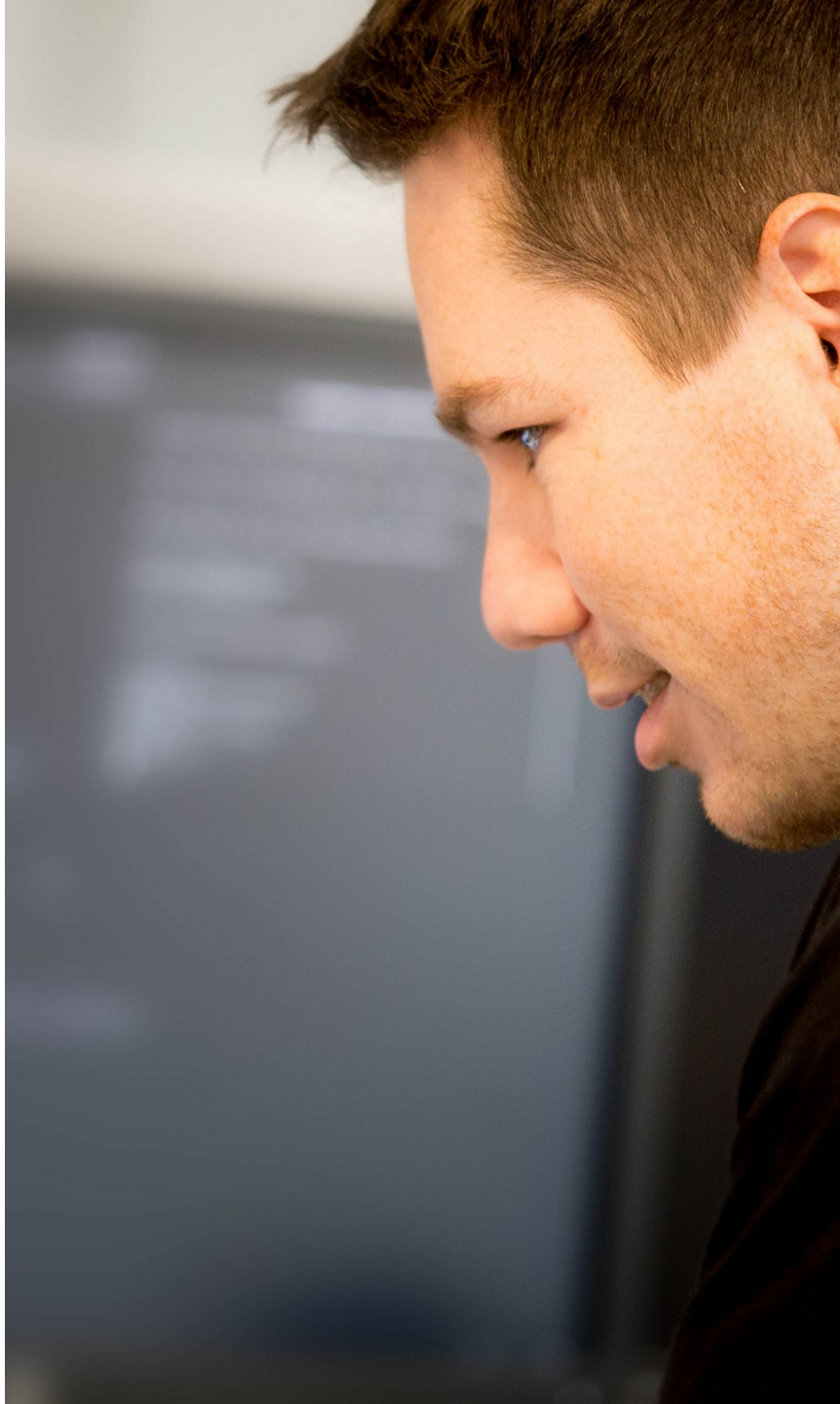
- M365-phishing
- Kredittkort-/BankID-phishing
- Webhotell

Vi har så langt i år jobbet med flere sakskomplekser hvor virksomheter har vært utsatt og rammet av propagerende phishingkampanjer, inkludert kampanjer som fisker flerfaktor. Med propagerende mener vi at når en konto er kompromittert, vil trusselaktøren bruke tilgangen til å sende nye phishingangrep til adresser den aktuelle kontoen allerede har vært i kontakt med – spesielt utsatt kan andre ansatte i egen virksomhet være. Vi er kjent med tilfeller hvor kontoer med høyere tilgangsnivå har blitt kompromittert i "runde to" i slike angrep. Det er kritisk å fange opp slike kompromitteringer så fort som mulig, ettersom tilgangen til, for eksempel, bedriftens M365-løsning, vanligvis eksponerer store mengder sensitive data til en trusselaktør, for eksempel alle e-poster brukeren har tilgang til, samt Teams, Sharepoint og OneDrive. Vi vet om tilfeller der informasjon fra og tilgang til e-postkontoer har bidratt til å gjennomføre svindler.

I disse sakene har vi delt IP-adresser brukt av trusselaktører for innlogging i M365, og vi anbefaler sterkt at alle både blokkerer IP-adressene for innlogging via Conditional Access-regler og søker etter IP-adressene i sine logger. Vi deler også IP-adresser brukt til denne typen phishing i blokkeringslistene våre, og vi har delt PowerShell-script for å automatisk søke etter disse i M365 samt å forhindre innlogging fra de. Dette ble omtalt i forrige månedsfokus, der opptak av webinaret ligger på nettsidene våre.

Vi har siden januar jobbet tett med andre SRM og tjenesteleverandører for å håndtere større runder phishingangrep der blant annet varemerker fra helsesektoren misbrukes. Innenfor dette området har vi gjort en del research, og har i flere tilfeller både avdekket og tatt ned phishinginfrastruktur tilhørende trusselaktører, også før denne er tatt i bruk i aktive kampanjer.

Vi ser også en økning i kompromittering av webhotell, der trusselaktør legger inn egne DNS-oppføringer hos offeret. Dette bruker de for å sende ut phishing-eposter gjennom tredjepartstjenester, og linke tilbake til et subdomene av offerets domene (eks "tracking.offer.no"). Her er det viktig å bruke flerfaktorautentisering på webhotell, fortrinnsvis phishingresistent autentisering, og dette blir viktigere i tiden fremover.



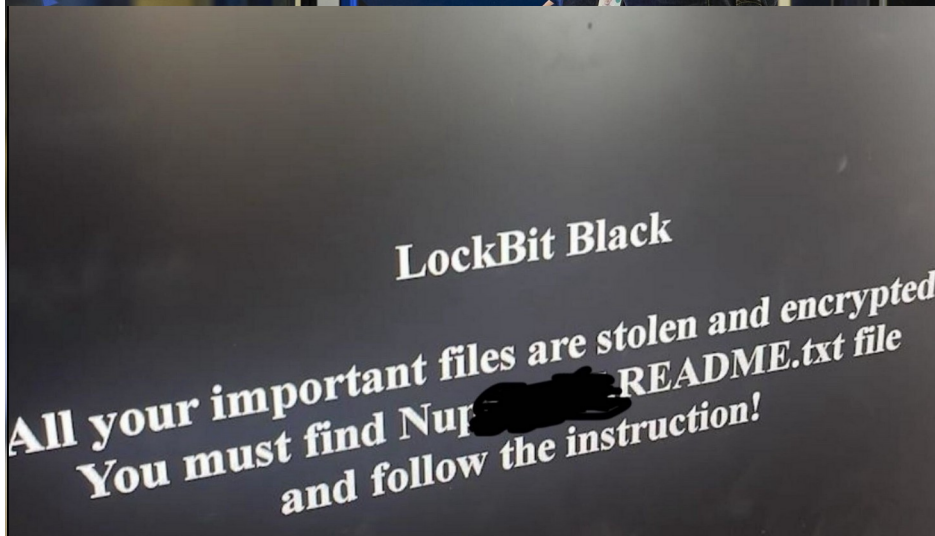
Hendelser siste tertial

Kryptert møteromsløsning

En virksomhet i kommunesektoren fikk sin møteromsløsning kryptert med ransomwarevarianten Lockbit Black. Løsningen ble administrert av en tredjepart via TeamViewer på en Windowsmaskin. Systemet skulle vært offline, men en konfigurasjonsfeil medførte at det var koblet til nett. TeamViewer var satt opp med "Easy Access", som innebærer at pålogging kun krevde TeamViewer-ID og passord. Analysen av hendelsen viser at systemet sannsynligvis hadde et lett gjettbart passord, og at angriperen, etter å ha forsøkt samme passord på tvers av en rekke TeamViewer-ID-er, tilfeldigvis fikk tilgang til det aktuelle systemet. Første tilgang til systemet skjedde midt i 2023, og det antas at den opprinnelige aktøren har videresolgt tilgangen. I februar ble programvaren XMRig installert for å utvinne kryptovaluta på systemet. I april ble systemet infisert med Lockbit Black. Hendelseshåndteringen er avsluttet, og det vurderes at omfanget var avgrenset og systemet tatt av nett.

Konkrete læringpunkter fra virksomheten som ble rammet:

- Windowsmaskinen var ikke kjent for driftsavdelingen
- Maskinen med TeamViewer skulle ikke vært koblet til nett
- Klientisolering manglet på gjestenettet
- Selve løsningen hadde ingen intern segmentering eller logging
- Da hendelsen inntraff ble maskinen slått av i stedet for å ta ut nettverkskontakten, noe som gjorde at man mistet verdifull informasjon for analyse, spesifikt muligheten for å ta minnedump
- Selskapet hadde mangelfull kontroll på konfigurasjon på utstyr levert og driftet av tredjepart



Hendelser siste tertial

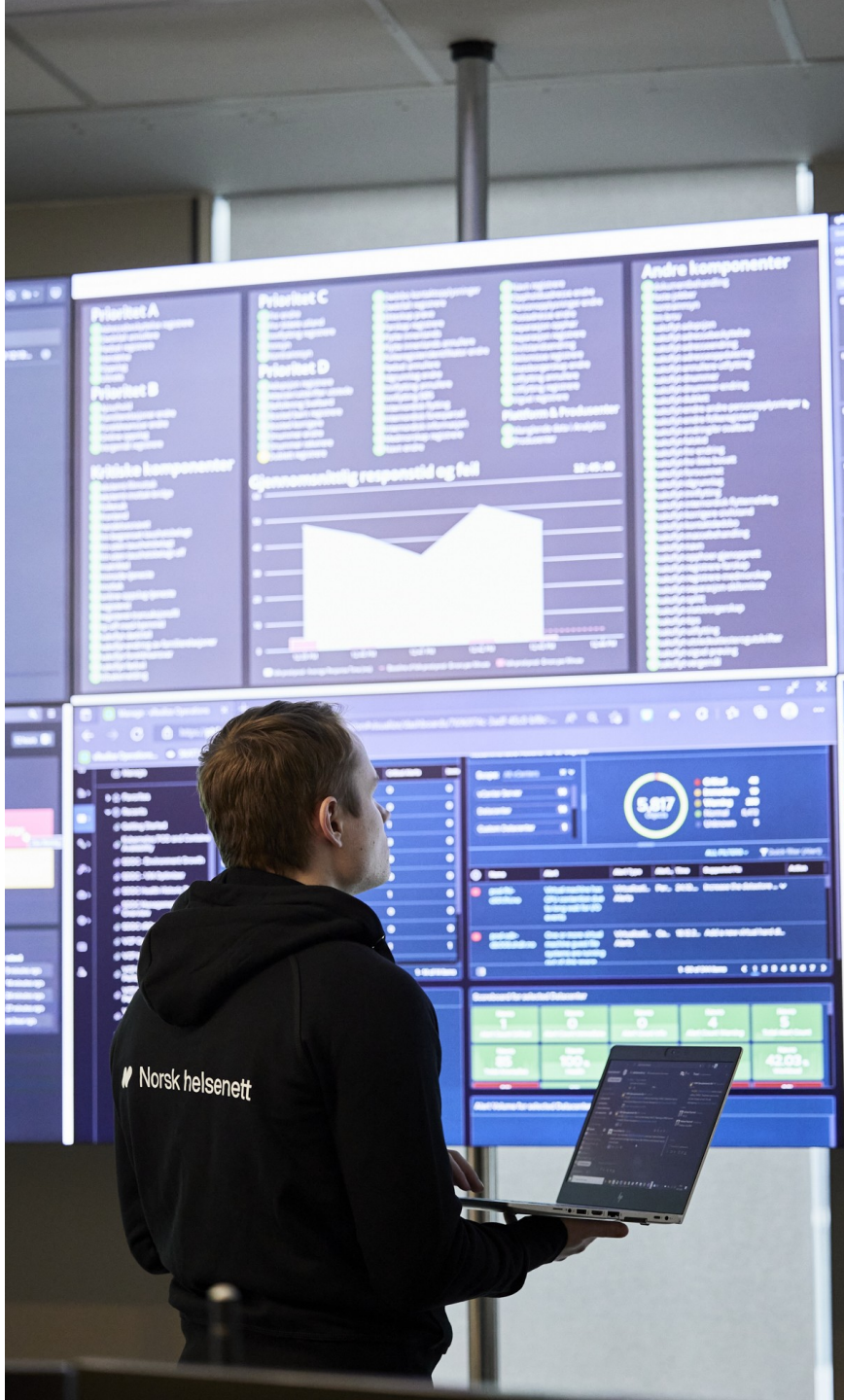
Kritiske sårbarheter i Internetteksponerte tjenester
De av dere som mottar rapporter fra sårbarhetsskanningen vår har kanskje fått en telefon fra oss de siste månedene - en stor del av ressursene våre har gått med til å følge opp kritiske sårbarheter i internetteksponerte systemer. Dette er for det meste nye sårbarheter vi varsler om idet de offentliggjøres. Fortinet, Citrix, Ivanti, ConnectWise, Palo Alto, og Cisco er eksempler på leverandører av produkter som har vært rammet siste tiden.

Det har det siste året vært en trend i at statlige aktører bruker store ressurser på å finne sårbarheter i systemer som er ment eksponert på internett, som VPN-mottak, og de siste tre månedene er ikke noe unntak. Vi ser at sårbarheter gjerne utnyttes av statlige aktører til spissede operasjoner, og når sårbarhetene blir offentlig kjent blir de utnyttet til massekompromitteringer. Ofte resulterer disse i krypterte systemer, eksfiltrert data, krav om løsepenger og om løsepenger ikke betales: publisering av stjålet informasjon.

I tilfellene der det ikke er såkalte 0-days som utnyttes, ser vi at *tiden fra* ***oppdateringer*** *som lukker sårbarheter* ***publiseres*** *av leverandør til de* ***utnyttes*** *av trusselaktører* fortsatt er på vei nedover. Det er derfor veldig viktig å ha muligheten til å oppdatere så raskt som mulig – man har ikke alltid tiden tilgjengelig til neste dag. Derfor etterspør vi kontaktinformasjon for tidskritiske henvendelser utenfor normal arbeidstid for virksomheter som ikke tidligere har oppgitt dette til oss. I tillegg har vi flere eksempler på at ulike leverandører oppdaterer først, og så senere annonserer at kritiske eller alvorlige sårbarheter ble lukket. Dermed blir det også viktig å oppdatere systemene både jevnlig og hyppig.

Vi ser dessverre at flere virksomheter fortsatt eksponerer administrasjonsgrensesnitt rett på internett, dvs. webgrensesnitt for å administrere for eksempel VPN-utstyr. Disse bør aldri være eksponert rett på nett, og vi anbefaler at slike tas ned så raskt som mulig. Vi henviser til tidligere webinar om angrepsflate og anbefaler samtlige virksomheter å eksponere kun det som er strengt nødvendig, og heller legge så mye som mulig bak VPN. Reduksjon av angrepsflate var vårt månedsfokus for februar.

Kompromitterte brukernavn og passord
Vi fikk tidligere i år tilgang til ca 11.400 brukernavn og passord på avveie som vi har varslet berørte medlemmer om. Varslingen vår er basert på informasjon vi har om domener som eies av de forskjellige virksomhetene i sektoren. Det er derfor derfor viktig at vi får tilbakemelding om endringer i domener for at dere skal få best mulig varsling fra oss.



Trusselen fra statlige aktører

Vi har tidligere rapportert at vi har sett at statlige trusselaktører med tilknytning til Russland og Iran har vært aktive mot helse- og kommunesektoren. Iran med gruppen Mint Sandstorm i en hendelse vi fortalte nærmere om i et webinar i september i fjor, og Russland med COLDRIVER som vi nevnte i situasjonsbildet vårt i 2022. Fra Russland har vi tidligere sett gruppene APT28 og APT29 aktive mot en eller flere av sektorene våre, og vi har også sett aktivitet fra Kina, da fra gruppen APT40. Vi er ikke kjent med aktivitet fra disse gruppene mot våre medlemmer i løpet av siste tertial.

Generelt ser vi at kapasiteten statlige aktører har til å gjennomføre angrep er høy, og kompetansen er økende.

Vi har den siste tiden sett flere tilfeller av større operasjoner fra statlige aktører, inkludert angrep mot og tydelig posisjonering i kritisk infrastruktur. Vi kan som eksempler nevne Volt Typhoon som ble godt beskrevet i en rapport fra CISA, og en annen antatt IRGC (Iranske revolusjonsgarden)-tilknyttet aktør, som kompromitterte et vannverk i Pennsylvania i USA. Angrepet medførte at vannverket måtte over på manuelle rutiner for å vedlikeholde vanntrykk ut til befolkningen.

Vi vurderer at tilsvarende tilganger i norsk kritisk infrastruktur er attraktivt for statlige aktører, og forventer også at det pågår aktivitet for å oppnå dette i dag.

Antall destruktive angrep fra statlige aktører har økt de siste årene, men i stor grad koblet til væpnede konflikter – Ukraina og Israel/Palestina.

Vi registrerer at flere statlige aktører har begynt å brukte kompromitterte hjemmerutere i angrep slik at trafikken ser ut som legitim hjemmebrukertrafikk. Dette vil f.eks. kunne omgå tiltak som geoblokkering. Geoblokkering vil fortsatt være effektivt for å forhindre masse-angrep og redusere støygulvet, men vil ikke være tilstrekkelig som tiltak alene. Dersom man skal implementere geoblokkering bør man som hovedregel stenge for alt, og bare åpne for det man vet man trenger, i stedet for å blokkere for der man tror man bør blokkere trafikk fra.

Trusselen fra organiserte kriminelle

Ransomware
Ransomwaregrupper og ransomwareaffiliates utgjør fortsatt den største trusselen mot IT-systemer med tanke på tilgjengelighet og konfidensialitet. Med ransomware tenker vi her både på kryptering av filer – og dermed systemer gjort utilgjengelig – og ren eksfiltrasjon av data og utpressing for å ikke publisere. Som vanlig har det vært flere større hendelser mot helsesektoren internasjonalt de siste månedene.

Av de største skal vi kort nevne Change Healthcare, som betalte rundt 22 millioner dollar (ca 235 million norske kroner) til AlphV-gruppen. Angrepet påvirket pasientbehandling på en litt annen måte enn det ville i Norge, ved at pengeflyten stoppet opp ettersom betalingsløsninger var utilgjengelige. Leverandøren Change Healthcare er involvert i rundt 1/3 av alle pasientjournaler ved sykehus i USA. Selv om systemer benyttet for å behandle pasienter ikke ble gjort utilgjengelige meldte 74% av rammede sykehus at angrepet hadde påvirket pasientbehandling.

Litt mer nærliggende og relevant er hendelsen i Dumfries og Galloway i Skottland i mars, der gruppen INC Ransom truer med å publisere 3 TB med data – dette inkluderer pasientjournaler. Her er vi ikke kjent med at hendelsen har fått store konsekvenser for pasientbehandling, men lekkasje av sensitive data er mer enn ille nok. INC Ransom er en av de ransomwareaktørene som har angrepet flest virksomheter internasjonalt i helsesektor så langt i år, kun forbigått av Lockbit.

Statistikk fra USA viser oss at under ransomwareangrep øker dødelighetsraten ved sykehus.

Vi fulgte TietoEvry-saken i januar tett da den påvirket flere svenske kommuner, selv om kommunene i seg selv ikke var målet. Mengden forskjellige løsninger i norske virksomheter – og spesielt kommuner – gir de en stor og variert angrepsflate, og det er kritisk å få oversikt over – og redusere – egen angrepsflate.

Svindel
Vi ser fortsatt direktørsvindler, men i mye mindre omfang – i hvert fall som rapporteres inn til oss – enn for noen år siden, og her virker trusselaktørene til å fortsatt bruke de samme teknikkene og metodene, og går ofte på kjøp av gavekort. Spesielt ser vi e-poster av typen fornavn.etternavn.domene@outlook.com - et angrep mot en virksomhet med domenet "offer.no" hvor angriper utgir seg for å være "Ola Nordmann", vil e-post-adresse benyttet for svindelen typisk være ola.nordmann.offer@outlook.com

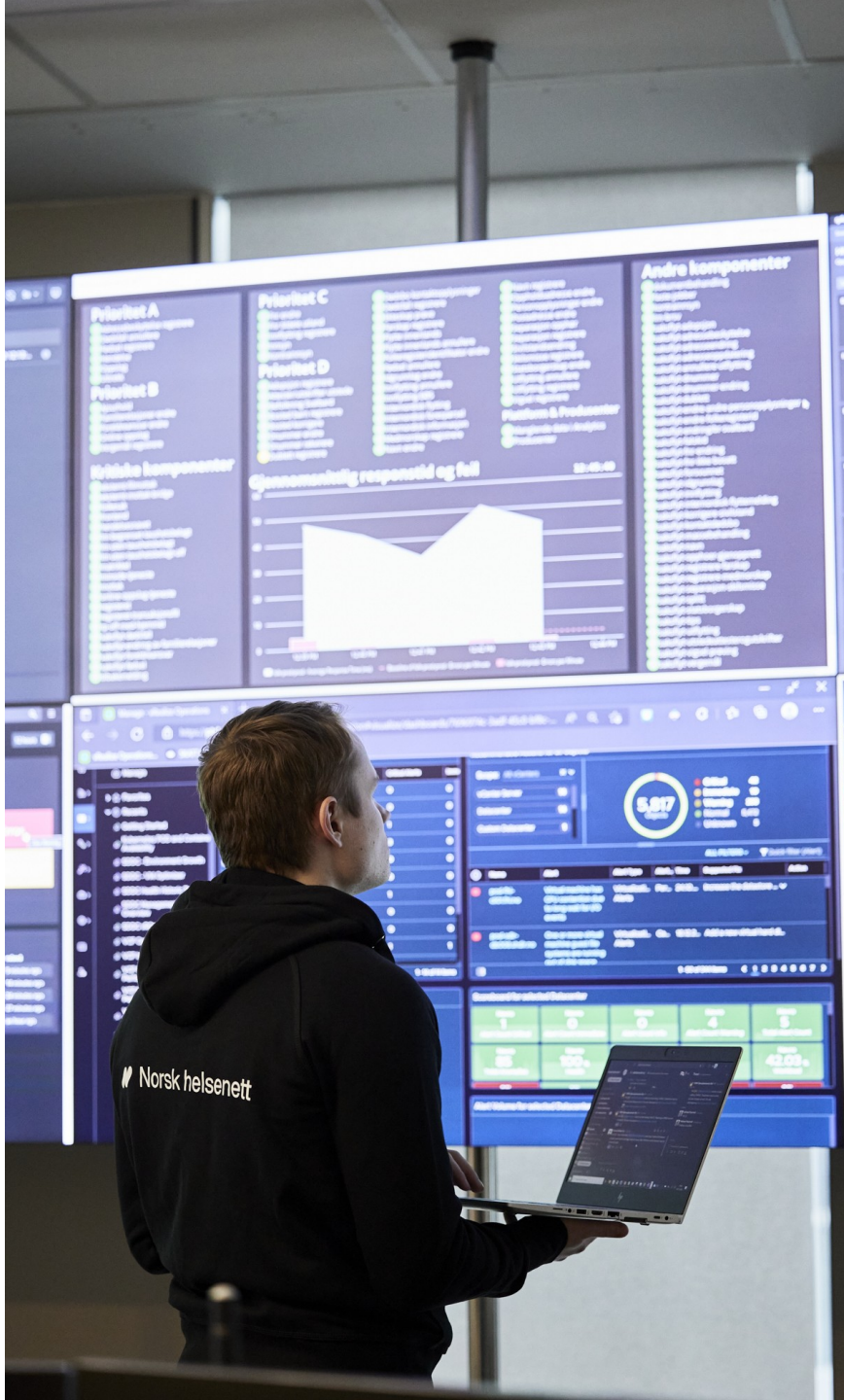
Trusselen fra hacktivister

Vi har sett lite aktivitet fra hacktivister mot helse- og kommunesektoren så langt i 2024.

Vi har fulgt trusselen fra pro-russiske hacktivister tett siden invasjonen av Ukraina i 2022. Basert på våre observasjoner, ser vi at deres fokus og hvilke mål de sikter seg inn på endrer seg raskt, og vi ser tette koblinger mellom mediesaker, endring i geopolitisk situasjonsbilde og prioriteringene til hacktivister.

Vi vurderer hacktivister til å utgjøre liten trussel mot helsesektor, men med et større potensiale for å påvirke kommunesektoren, da spesielt tilgjengelighet.

Vi ser at enkelte statlige aktører gjemmer seg bak hacktivistmerket og vi har sett flere indikasjoner på russiske statlige aktører har gjort det. Et annet eksempel er aktiviteten fra den pro-Iranske gruppen som kaller seg "Cyber Av3ngers" som sto bak angrepet på vannverket i USA nevnt tidligere. De har knytninger til den Iranske Revolusjonsgarden.



Trusselvurdering

Vårt situasjonsbilde uendret i løpet av siste tertial og er publisert på våre nettsider.

- Det er meget sannsynlig at fremmede stater ser på helsesektoren som et mål for spionasje.
- Vi mener det er sannsynlig at norsk helse- og kommunesektor vil treffes av angrep fra aktører som et ledd i det generelle arbeidet til statlige eller stats-sponsede etterretningstjenester.
- Vi mener det er meget sannsynlig at norsk helse- og kommunesektor vil treffes av angrep fra organiserte kriminelle grupper.
- Vi mener det er meget sannsynlig at norsk helse- og kommunesektor vil treffes av angrep fra hacktivister. Typisk tjenestenektangrep.

Anbefalinger

- Implementer phishingresistent autentisering på eksponerte tjenester
  - Spesielt viktig på M365
- Lukk sårbarheter som er rapportert i vår sårbarhetsoversikt
  - Meld eventuelle falske positiver tilbake til oss på post@helsecert.no
- Gå gjennom portskannrapporten vår og fjern unødvendige tjenester
  - Tjenester som ikke burde vært eksponert og/eller ikke lenger blir driftet blir oftest kompromittert
- Kjør vår Hurtigtest for cybersikkerhet
  - Ved å sende resultater inn til oss spiller dere oss gode
- Sørg for at våre kontaktpunkter hos dere er riktig og oppdatert
  - Se oversikt i e-posten denne rapporten kom i

Norsk helsenett

Helse- og KommuneCERT

Tilbakeblikk 1. tertial 2024

post@helsecert.no