Norsk helsenett
Helse- og kommuneCERT

Tertialsbrief T3 2025

Situasjonsbilde

Overordnet

Vi bygger vårt situasjonsbilde basert på informasjon vi har tilgjengelig til enhver tid. Denne kommer fra medlemmer, samarbeidspartnere og andre eksterne kilder som sikkerhetsselskap og sikkerhets- og etterretningstjenester.

Dette situasjonsbildet har det siste året holdt seg statisk uten nevneverdige endringer.

I tredje tertial 2025 ble flere norske kommuner truffet av tjenestenektangrep under Storting- og Sametingsvalget. Dette var et forsøk fra pro-russiske hacktivister på å ramme Norge og tyder ikke på at norske kommuner er av spesiell interesse for hacktivister, kun at Norge som land og norsk infrastruktur er av interesse.

Vurderinger

- Det er meget sannsynlig at fremmede stater ser på helsesektoren som et mål for spionasje.
- Det er meget sannsynlig at fremmede stater ser på kommunesektoren som et mål for spionasje og påvirkningsoperasjoner.
- Det er sannsynlig at norsk helse- og kommunesektor vil treffes av angrep fra aktører som et ledd i det generelle etterretningsarbeidet til fremmede stater.
- Det er meget sannsynlig at norsk helse- og kommunesektor vil treffes av angrep fra organiserte kriminelle grupper.
- Det er mulig at norsk helse- og kommunesektor vil treffes av angrep fra hacktivister.

Vurderinger - forenklet

- Medlemmene våre vil bli utsatt for spionasje- og påvirkningsoperasjoner.
- Medlemmene våre er attraktive mål for organiserte kriminelle.
- Hacktivister har ingen spesiell interesse i medlemmene våre.

Norsk helsenett
Helse- og kommuneCERT

Hendelser

Tjenestenektangrep mot norske kommuner

Mandag 1. september annonserte en pro-russisk hacktivistgruppe at de skulle angripe Norge. De publiserte en melding på Telegram-kanalen sin der de viser til at Russland og styrking av NATO har vært et hovedfokus i norsk valgkamp. Dette ble presentert som motivasjon for å angripe Norge og norsk infrastruktur i dagene før Stortings- og Sametingsvalget 2025.

I uken før valget angrep gruppen forskjellige mål i Norge. Kommuner, politiske parti og Stortinget var blant målene som ble rammet gjennom uken. Vår vurdering var at helsesektoren ville forbli urørt, men at kommunene måtte forvente å se aktivitet gjennom uken.

Tjenestenektangrepene stoppet på valgdagen, og gruppen rettet fra da av fokuset mot Frankrike og Ukraina i stedet for Norge.

Denne og lignende grupper er mer opptatt av oppmerksomhet og å bygge opp sin egen merkevare enn av reell konsekvens, og velger ofte vilkårlige mål.

Vi er ikke kjent med konsekvenser av angrepene utover mindre nedetid (minutter) på nettsider.

Pro-russiske hacktivister

Pro-russiske hacktivister har angrepet mål i Norge jevnt og trutt siden den russiske eskaleringen i krigen mot Ukraina 24. februar 2022. De siste fire årene har vi sett flere typer angrep fra grupper vi klassifiserer som hacktivister. I løpet av 2025 så vi en endring i målutvelgelse og typen angrep fra disse gruppene. De klassiske angrepene fra pro-russiske hacktivister har vært tjenestenektangrep – angrep som har som formål å gjøre nettsider utilgjengelige. De fleste angrep fra hacktivister har vært av denne typen, og har hatt begrenset konsekvens for ofrene.

Gjennom 2025 så vi en økning av angrep mot internetteksponerte OT-systemer fra disse gruppene. Flere grupper begynte å annonsere at de har kompromittert OT-systemer og publisert video og bilder som bevis.

Mot slutten av 2025 etablerte det seg en stigende trend på at pro-russiske hacktivister publiserte bilder og videoer fra webkamera i forskjellige land. Bilder og videoer blir publisert sammen med provoserende tekster rundt landets ledelse, ofte også med negative karakteristikker av landets befolkning, og oppfordring til drap, bombing og voldtekt..

ClickFix

I 2025 så vi en kraftig økning i bruken av ClickFix. ClickFix er en sosial manipulasjonsmetode hvor offer lures til å kopiere og kjøre en angriper-styrt kommando på egen maskin. Antall ClickFix-angrep verden over mangedoblet seg fra 2024 til 2025, og vi så videre utvikling i metoden mot slutten av 2025.

FileFix

Der ClickFix ber brukeren åpne enten «Run»-dialogen eller en terminal, ber FileFix brukeren åpne Windows Filutforsker og lime inn en tekststreng i adressefeltet. Denne strengen er, som med tradisjonell ClickFix, en ondsinnet kommando, ofte PowerShell, som gir angriper kontroll på maskinen om den kjøres.

ClickFix brukes av statlige aktører

Flere statlige aktører bruker ClickFix og ClickFix-lignende teknikker i angrepene sine. I 2025 har man sett metoden brukt av statlige nordkoreanske, iranske og russiske trusselaktører, av og til innlemmet som et verktøy i eksisterende angrepsoperasjoner.

Vi ser ingen grunn til at bruk av ClickFix og lignende metoder vil forsvinne. Metoden er klassisk sosial manipulering, og fungerer, så metodene vil være aktuelle for en angriper så lenge brukere har lov til å kjøre programmer og kommandoer.

VA/OT-funn i Norge

Gjennom siste tertial i 2025 jobbet vi målrettet for å avdekke internetteksponerte OT-systemer i Norge. Resultatene var nedslående, og vi fant flere hundre systemer som var direkte eksponert på internett med enten svakt passord eller fabrikkpassord, eller helt uten passord.

Typen systemer vi har avdekket strekker seg fra byggtekniske systemer til systemer tilknyttet vannforsyning og kraftverk. For systemer tilhørerende våre medlemmer varsler vi direkte til virksomheten. For andre systemer varsler via fortrinnsvis via relevant sektorvis responsmiljø. Det er dessverre mange systemer vi ikke har klart å identifisere eier av og som ikke har blitt varslet.

Brukernavn og passord på avveie

I siste tertial har vi avdekket større mengder brukernavn og passord på avveie hos medlemmene våre.

I forrige tertial varslet vi medlemmene våre om over 25 000 kompromitterte passord, mens for hele 2025 er tallet over 100 000. Disse er koblet til henholdsvis 17 000 og 55 000 unike brukernavn.

Passordene kan være stjålet lenge før vi finner ut av det og får varslet dere. Når vi får vite om det er det som regel allerede delt med flere andre aktører, og kan være brukt av angripere. Det er derfor viktig å reagere raskt på slike varsel fra oss.

Vi får ikke med oss alle passord som stjeles, så dere må ta utgangspunkt i at dere har passord på avveie uten at dere får beskjed fra oss. Dette understreker viktigheten av sikringstiltakene AD-tiering og phishingresistent autentisering.

Adversary-in-The-Middle-phishing

Gjennom 2025 har vi sett et vedvarende høyt nivå av Adversary-in-The-Middle-phishing (AiTM) mot våre medlemmer. Vi estimerer at det har gått rundt en kampanje i uken i snitt mot medlemmene våre. Dette har resultert i rundt tre kompromitteringer hver uke. Om vi ekstrapolerer for hele Norge vil tallet være minst ti-gangen, men her er det store mørketall.

Medlemmene våre er flinke til å melde inn AiTM-phishing til oss, noe som både gir oss god oversikt og gjør at vi får stoppet spredning raskere. Sammen med medlemmene våre, samarbeidspartnere som Nordic Financial CERT (NFCERT) og Næringslivets Sikkerhetsråd (NSR) bidrar vi til å forhindre flere kompromitteringer i Norge hver dag.

Anbefalinger

Sikre OT-utstyr

OT-utstyr bør som hovedregel aldri eksponeres direkte på internett. Dessverre gjøres dette i utstrakt grad, og vi finner ofte utstyr eksponert med utilstrekkelig sikring. Fabrikkpassord og manglende multifaktorautentisering er en gjenganger, også på grensesnitt der man kan *kontrollere* fysiske prosesser og ikke bare overvåke.

Dette er ikke godt nok i 2026. OT-utstyr bør beskyttes bak VPN, med sterke passord og – om mulig – multifaktorautentisering.

Phishingresistent autentisering

Om man ikke har innført phishingresistent autentisering for sentrale internetteksponerte tjenester enda er det bare å begynne. Adversary-in-The-Middle-phishing er ikke på vei bort, og om man ikke er rammet av det enda er det bare et spørsmål om tid. Sentrale tjenester hos leverandører som Microsoft, Google og Okta er kontinuerlig mål for AiTM-phishing og er tjenester som absolutt bør beskyttes med phishingresistent autentisering.

Slike tjenester kan ofte brukes som single-sign-on-løsning for andre tjenester, som da også blir bedre beskyttet om man innfører phishingresistent autentisering.

AD-tiering

Vi anbefaler sterkt at man innfører AD-tiering for å redusere konsekvensen dersom en angriper kommer på innsiden. I juni 2025 holdt vi en webinarserie om AD-tiering som vi anbefaler å se dersom man vil sette seg inn i temaet.

Sjekk angrepsflaten jevnlig

Det kan være vanskelig å vite nøyaktig hva man har eksponert på internett til enhver tid, og derfor anbefaler vi at man sjekker dette jevnlig. Dette gjelder spesielt etter større endringer, som endringer i tjenesteleverandører og bytte av eller oppdatering av sentrale nettverksenheter som brannmurer. Dersom man allerede har en god oversikt over IP-adresser og domener har man allerede et godt utgangspunkt for å verifisere at kartet stemmer med terrenget.

Oversikt over IP-adresser, domener og utstyr

Hver virksomhet må passe på å ha en oppdatert oversikt over IP-adresser og domener de bruker. Det samme gjelder utstyr som er eksponert på internett. Uten en god oversikt over hva man selv har kommer man utrolig skjevt ut når man skal håndtere sikkerhetshendelser som kritiske sårbarheter eller kompromitteringer.

Oversikt over IP-adresser og domener bør sendes til oss, sammen med en oppdatert liste over kontaktpersoner – inkludert et vakt-kontaktpunkt som kan nås 24/7 ved kritiske hendelser.

Fjern eksponering av tjenester som ikke må være eksponert

Tjenester som ikke har et behov for at man kan nå de fra internett bør legges bak brannmur. Selv om det i dag ikke er en kritisk sårbarhet i tjenesten som utgjør en trussel, så ser vi igjen og igjen at sårbarheter dukker opp og blir utnyttet på få dager. Vi så dette senest rundt juletider, der en sårbarhet i MongoDB ble publisert lille julaften og utnyttet 2. juledag, tre dager senere.

Begrens utkoblingsmuligheter

Hvor mulig bør man begrense utkoblingsmuligheter fra kantenheter som VPN-mottak, brannmurer og lignende. Dette for å sikre at en angriper ikke like lett får kontroll på enheten gjennom en sårbarhet.