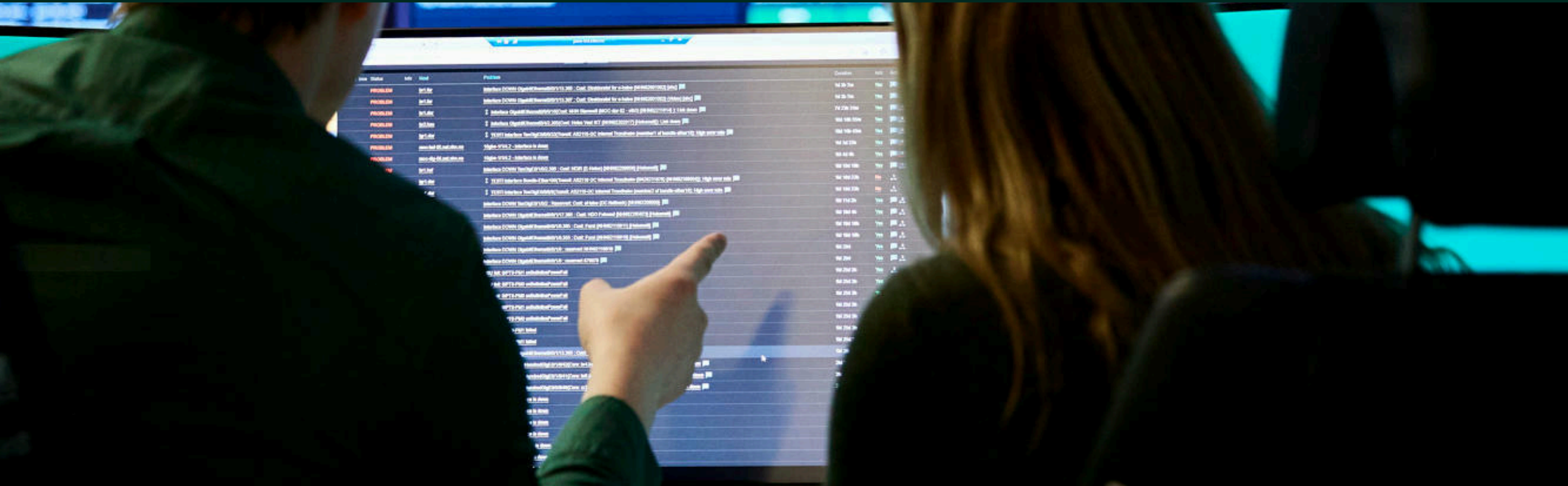


Tilbakeblikk 2. tertial 2026

Helse- og kommunesektoren



Innholdsfortegnelse

 Nytt fra Helse- og kommuneCERT	3
 Vakttelefon og Medlemsportal	3
 Skytest og Hurtigtest	4
 Medlemsherding	5
 Situasjonsbilde	6
 Hendelser	7
 Trender	8

```
2 import { Modal, Popup, Form, Button } from "semantic-ui-react";
3 import {
4   faPlusCircle,
5   faQuestionCircle,
6 } from "@fortawesome/free-solid-svg-icons";
7 import { FontAwesomeIcon } from "@fortawesome/react-fontawesome";
8 import {
9   createErrorFields,
10  sortOptions,
11  optionifyCollection,
12 } from "@common/helpers";
13 import {
14  useCustomerFormReducer,
15  addOrgActionCreator,
16  setCustomerActionCreator,
17  setChildOrgsActionCreator,
18  setFormModeActionCreator,
19  setParentOrgActionCreator,
20  setDisplayNameActionCreator,
21  setOrgsActionCreator,
22 } from "../hooks/useCustomerFormReducer";
23 import { groupOptions } from "../constants";
24 import { set, setWith } from "lodash";
25 import {
26  AtlantisStateProps,
27  CustomerGroup,
28  CustomerItem,
29  InputHandler,
30  CheckboxHandler,
31  OrgNumber,
32 } from "@types";
33 import { ToolTipLabel } from "../FieldLabels";
34 import {
35  cancelFormActionCreator,
36  cancelFormAndPreserveActionCreator,
37 } from "@baseReducer";
38 import { useOrgNumberFields } from "../hooks/useOrgNumberFields";
39 import { useItemPost, useItemPut } from "../mutations";
40 import { useUnselectedCustomers } from "@cmdb/selectors";
```

Nytt fra Helse- og kommuneCERT

Vakttelefon

Vi har opprettet en vakttelefon med nummer **+47 40 03 50 31**.

Nummeret går direkte til oss og bemannes 24/7. På hverdager mellom 08:00 - 15:30 når du dagvakt, ellers kommer du til (hvilende) bakvakt.

Vi vil også bruke dette nummeret for å ringe ut. Vi anbefaler at dere lagrer nummeret både for å se hvem som ringer, og for å ha nummeret for hånden om dere har en hendelse.

OBS! Nummeret støtter ikke å motta SMS.

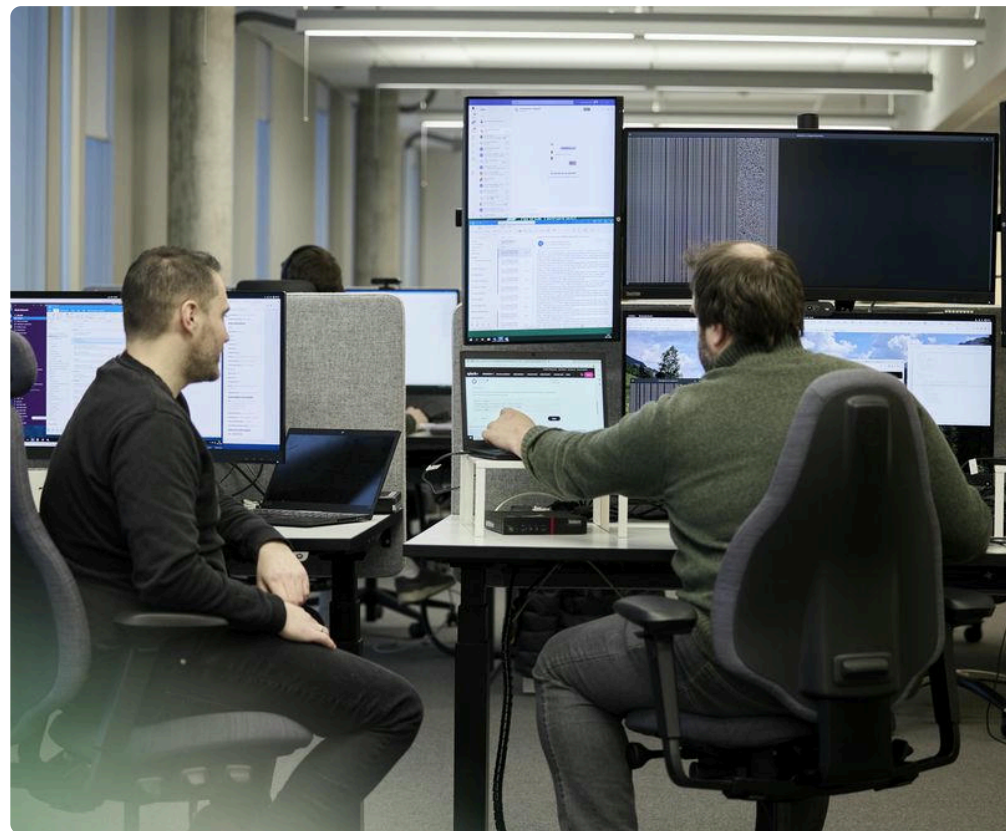
Medlemsportal

Dere kan nå logge inn i portal.helsecert.no. Her kan dere se og administrere egen informasjon. Portalen utvikles kontinuerlig, så forvent endringer.

Første gang du logger inn må du bruke ID-porten. Deretter kobler du kontoen som er opprettet i portalen med jobb-e-post og legger inn en eller flere [passnøkler](#) for videre tilgang.

ID-porten sikrer at identitet stemmer, riktig e-post knytter deg til riktig virksomhet og passnøkler sikrer mot phishing i fremtiden. Passnøklerne gjør også innloggingsprosessen vesentlig raskere.

Administrerer dere mer enn en virksomhet, kan dere be om tilgang til flere med samme bruker.



Nytt fra Helse- og kommuneCERT

Hurtigtest

Hurtigtest versjon 8.3 ble lansert 5. juni.

Nyeste versjon har en rekke nye sjekker både på **legacy-protokoller** og usikre innstillinger, samt lærdommer fra hendelsen hos Lørenskog kommune. **Ett eksempel på dette er om Notisblokk er satt som standardprogram for åpning av skriptfiler.**

Vi anbefaler at Hurtigtest kjøres minimum tre ganger i året.

[Full endringslogg](#)

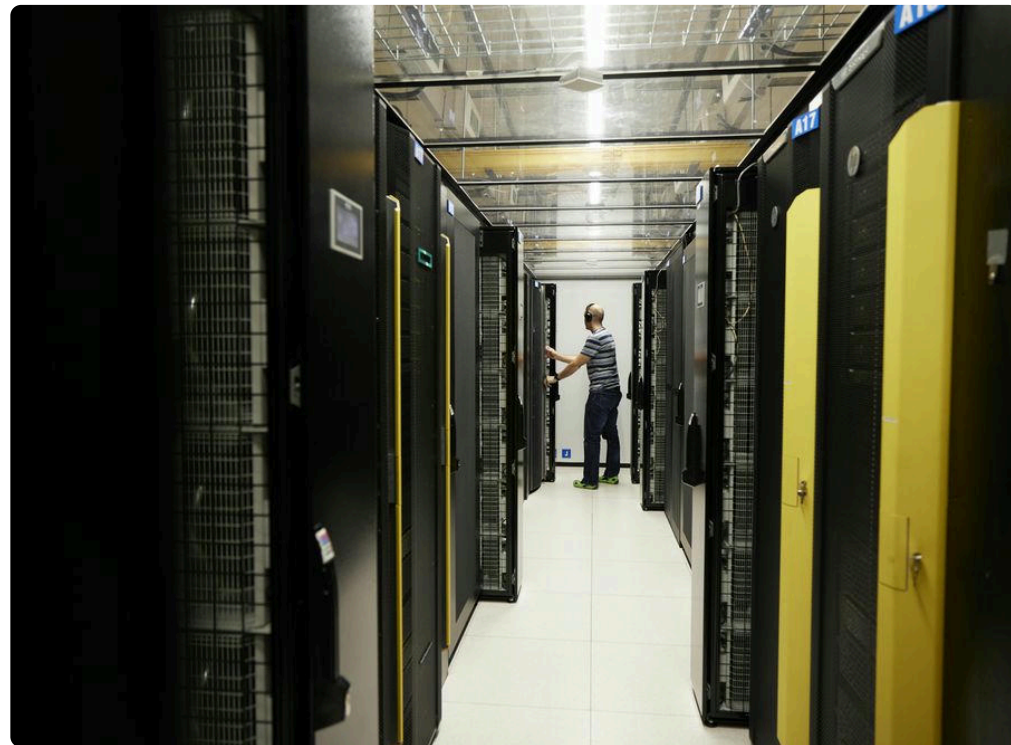
Skytest

Skytest versjon 1.5 ble lansert 8. juni.

Den gir nå en oversikt over **Conditional Access Policy**. I tillegg sjekker den om **device code flow** er tillatt (det bør kun være unntaksvis tillatt ref [webinar 20.03.2026](#))

Vi anbefaler at Skytest kjøres minimum tre ganger i året.

[Full endringslogg](#)



Medlemsherding

Sikringen medlemsherding gir er kjempeviktig. Uansett hvor god skallsikring man har vil det før eller siden skje en hendelse. Da er det sikringsgraden og flaks som avgjør hvor ille det blir.

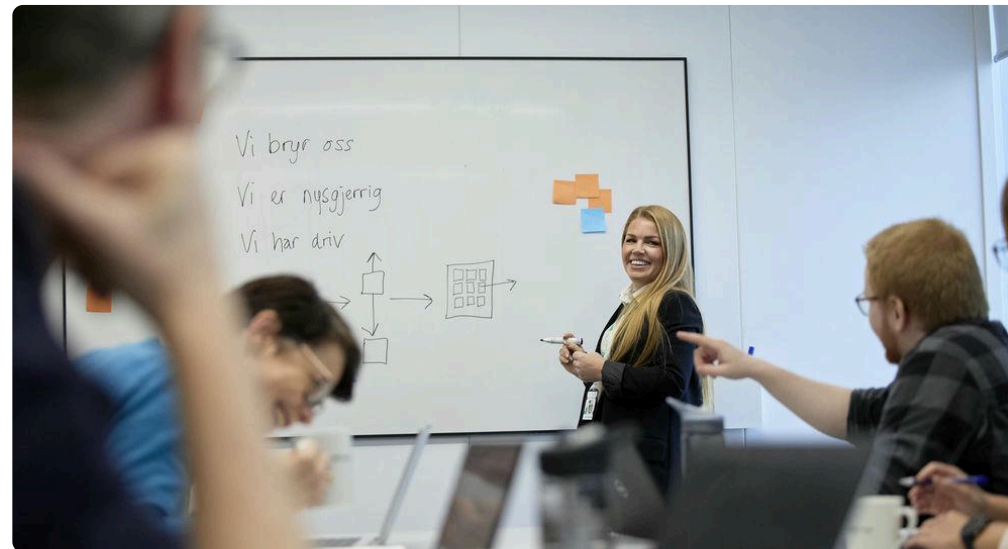
Medlemsherding gjør at dere ikke er avhengige av flaks.

Medlemsherding bygger på erfaringer fra mange hundre inntrengingstester og flere år med reelle hendelser og sikrer at de grunnleggende tiltakene er på plass. Gjennomført herding gir betydelig motstandskraft om du får en angriper på innsiden.

Medlemsherding er rettet mot Microsoft-baserte miljøer, både on-prem gjennom [Hurtigtest](#) og PingCastle, og skyløsninger gjennom [Skytest](#).

Vårt mål er at alle medlemmer med on-prem eller skyløsninger fra Microsoft gjennomfører Medlemsherding.

For spørsmål og svar om medlemsherding se [portalen](#).



Risikonivå og situasjonsbilde

Risikonivå

Vårt forenklete risikonivå står akkurat nå på **medium**.

Begrunnelsen for medium er:

- Store mengder kompromitterte norske nettsider som leverer skadevare gjennom teknikken som kalles ClickFix og varianter av ClickFix
- Det fortsatt store trykket phishing som omgår klassisk MFA
- Erklæring av cyberkrig mot norske myndigheter fra en pro-russisk hacktivistgruppe
- Mengden ransomwareangrep sett både i Norge og internasjonalt

Overordnet situasjonsbilde

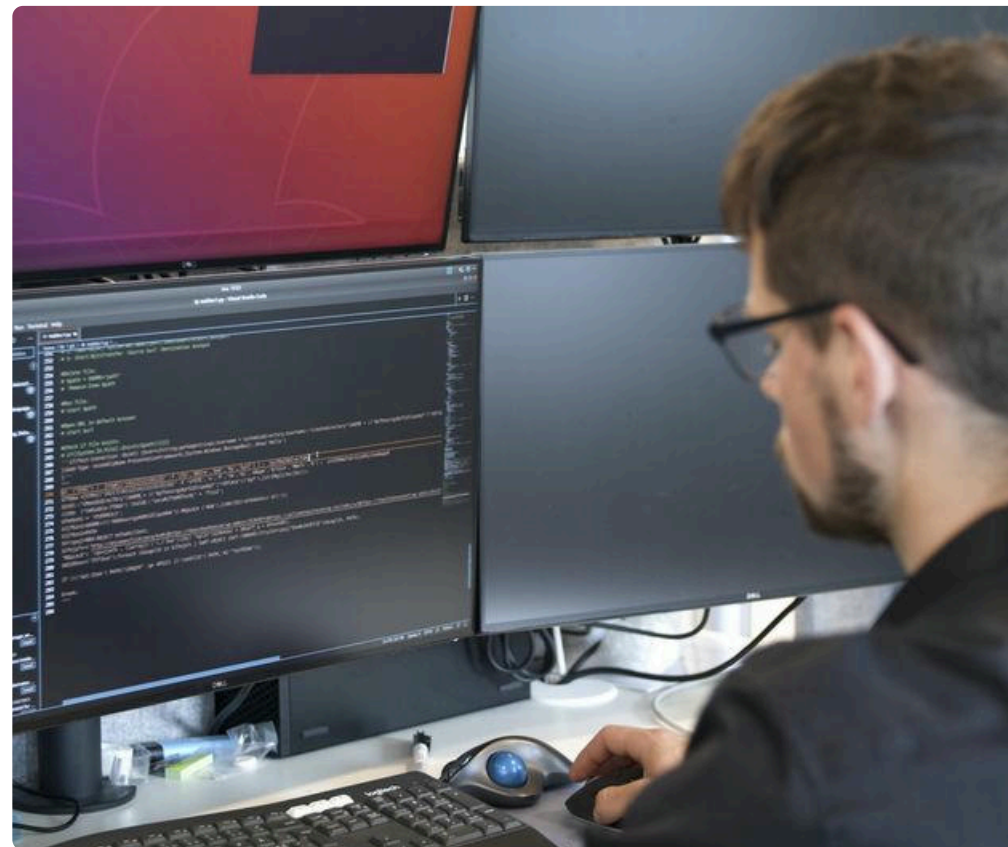
Medlemmene våre vil bli utsatt for spionasje- og påvirkningsoperasjoner.

Medlemmene våre er attraktive mål for organiserte kriminelle, som også resten av Norge er.

Hacktivistene har ingen spesiell interesse i medlemmene våre, men dette kan endre seg fort.

Vi så dette i fjor høst i uken før Stortings- og Sametingsvalg, og vi så det nettopp med en erklæring av såkalt «cyberkrig».

Dette er de forenklete vurderingene vi publiserer på [nettsidene våre](#), og er uendret fra forrige tertial.



Hendelser

Løsepengeangrep hos Lørenskog kommune

Som kjent ble Lørenskog kommune utsatt for et løsepengeangrep i mai i år. Angrepet startet med at en maskin ble kompromittert da en ansatt søkte etter noe på internett, fikk et SEO-manipulert resultat og ble servert skadevare forkledd som et dokument.

Skadevaren ble kjørt da brukeren åpnet «dokumentet», og dette ble ikke fanget opp av verken antivirus eller endepunktbeskyttelse. Dette gjorde at angriper fikk fotfeste i nettverket til Lørenskog kommune og kunne bevege seg videre.

Lørenskog kommune var allerede i gang med et sikringsløp for klienter, og av 3000 klienter var det rundt 200 som gjenstod. Den kompromitterte klienten var en av disse 200.

Vi henviser forøvrig til Lørenskogs utmerkede [informasjonsside om hendelsen](#).

Vi har noen generelle anbefalinger til tiltak basert på hendelsen.

1. [Åpne skriptfiler i teksteditor](#).

Sett standardhandlingen når brukerne dobbeltklikker på en skriptfil til å åpne den i for eksempel Notisblokk, i stedet for at filen kjøres.

2. [Gjennomfør Medlemsherding](#) fra Helse- og kommuneCERT.

Lørenskog kommune var allerede i gang med et sikringsløp, og det var blant de 200 klientene som gjensto at angrepet kom inn. Medlemsherding får på plass de grunnleggende tiltakene som stopper nettopp den bevegelsen videre i nettverket. Tjenesten er beskrevet på Medlemsherding-sliden.

3. Begrens trafikk ut fra servere og containere.

En intern databaseserver eller container trenger sannsynligvis ikke å nå eksterne nettsider som NRK eller VG. Trafikk fra servere og containere bør hvitelistes, altså at man skal eksplisitt tillate nødvendig trafikk.

4. [Backup](#) er kritisk for gjenoppretting!

Ha sikkerhetskopi, og ha den et sted angriper ikke kan nå den. Typisk for løsepengeaktører er at de går målrettet etter backupløsninger, nettopp for å sette virksomheten i en større skvis. Ha denne off-site, hos en ekstern leverandør eller lignende. Det viktige er at angriper ikke når backupen fra virksomhetens IT-nett, ev. ikke kan overskrive den. En write-once-løsning kan fungere. Lørenskog kommune hadde backup på plass, og det hjalp dem mye i gjenopprettingen.

Tjenestenektangrep mot ID-porten

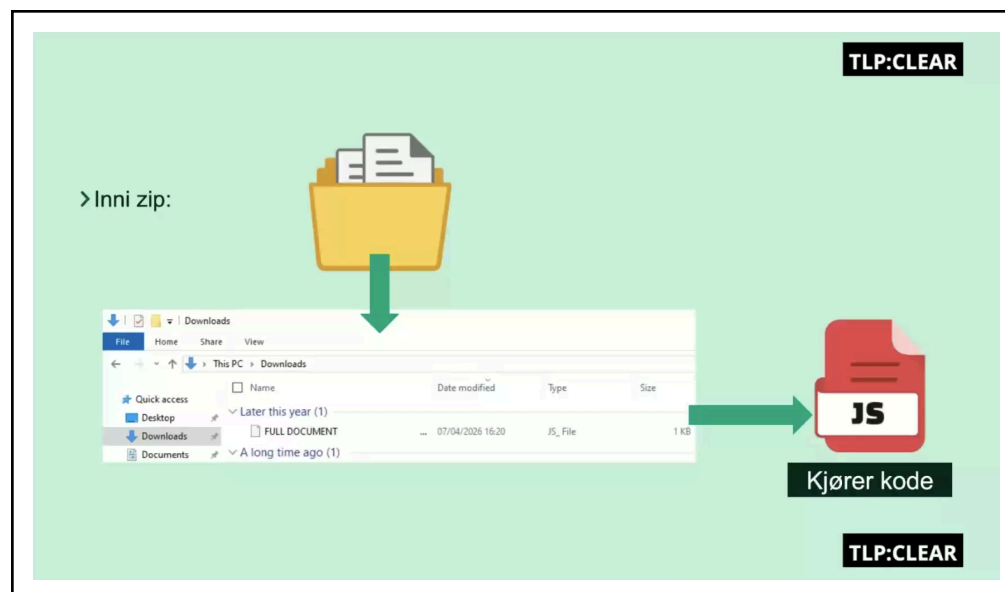
Gjennom sommeren ble ID-porten utsatt for tjenestenektangrep i to store runder, og mot slutten av august kom en tredje runde. Angrepene førte til at ID-porten var utilgjengelig i lengre perioder og gjorde at tjenester som var avhengig av ID-porten heller ikke kunne brukes. Så langt har ingen aktører tatt ansvar for angrepene.

Kompromittering av kompetansebroen.no

Kompetansebroen, som driftes av Ahus, er en portal for kompetansedeling og kurs i helsetjenesten, og portalen har vært utsatt for et angrep.

Som et sikkerhetstiltak blir alle brukere bedt om å bytte passord. Ahus opplyser at løsningen har ca. 100 000 brukere.

Ahus har en god [informasjonsside om hendelsen](#).



Angrepsforløp på klient, fra [webinaret om hendelsen hos Lørenskog kommune](#).

Trender

Kompromitterte norske nettsider

Det siste tertialet har vi hatt økt fokus på ClickFix. Vi oppdager stadig flere kompromitterte nettsider i Norge som brukes til å spre skadevare gjennom denne og beslektede teknikker, også i sektorene våre.



Vi koordinerer håndtering av disse med de andre sektorvise responsmiljøene (SRM-er). Her gjør Næringslivets Sikkerhetsråd (NSR) en formidabel jobb med varsling til mindre virksomheter. Som et eksempel på omfanget fant vi over 200 webkompromitteringer i Norge i løpet av en uke i august.

Gjennomgående for flere av disse kompromitteringene er manglende oppdatering av systemer som WordPress og Joomla, samt rammeverk som Next.js. Vi ser også at flere har enfaktorinnlogging, altså kun krever passord. Manglende flerfaktorautentisering gjør det lett å utnytte brukernavn og passord på avveie.

Volumet vi ser av kompromitterte nettsider i Norge gjør at du må forvente at brukerne dine blir utsatt for ClickFix-angrep, og ha på plass tekniske tiltak som reduserer sjansen for at de er vellykket.

Phishing som omgår klassisk MFA

Phishing som omgår klassisk MFA, slik som adversary-in-the-middle og Device Code Phishing, pågår i stor skala mot norske brukere. At brukerne dine blir utsatt for slik phishing er nå en del av normalsituasjonen.



Løsningen er det vi kaller «solid innlogging», som du finner mer informasjon om på [nettsidene våre](#). Hvis det ikke er mulig å innføre solid innlogging, bør dere som et absolutt minimum bruke blokkeringslistene våre og sperre for innlogging fra IP-adresser i dem. Dette vil forhindre en del av angrepene, men vil aldri kunne ta alt.

Økning i antall sårbarheter

Vi har generelt det siste året merket oss en økning i antall sårbarheter vi må vurdere for varsling mot medlemmene våre. En mulig årsak til det er at flere og flere bruker AI for å finne sårbarheter i mye brukt programvare.



Noen sårbarhetsrapporter er gode. Mange er dårlige, og baserer seg på veldig teoretiske konsekvenser som er usannsynlige eller i hvert fall ikke bevist mulige.

Det varsles i det hele tatt om langt flere sårbarheter enn før, noe som også betyr at vi håndterer kritiske sårbarheter hos medlemmene våre oftere.

Dette øker presset på oss med å vurdere slike sårbarheter, ofte på mangelfullt grunnlag. Samtidig øker det også presset på dere som må oppdatere systemene.

Derfor blir det stadig viktigere å redusere angrepsflaten så mye som mulig.

For å identifisere tjenester eksponert mot internett er portskannrapporten vi sender ut et godt utgangspunkt. Denne sendes ut månedlig, og inneholder både hva som er nytt siste måned, hva vi ikke ser lenger og totalen av identifiserte tjenester.

Tjenestenektangrep mot Norge

I tillegg til angrepene mot ID-porten erklærte en pro-russisk hacktivistgruppe «cyberkrig» mot norske myndigheter. Vår vurdering er at denne gruppen ikke sto bak angrepene på ID-porten.



I dagene etter erklæringen ble flere virksomheter i Norge truffet av tjenestenektangrep, blant annet Vy, Posten, flere mål i utdanningssektoren og andre statlige nettsider.

Disse angrepene har vært kortvarige, og typisk blitt avsluttet når de ikke lenger har synlig effekt på nettsiden eller etter at angriperne har rukket å ta et skjermbilde av den utilgjengelige nettsiden til følgerne sine.

Se også vår [guide for anbefalte sikkerhetstiltak knyttet til DDoS-beskyttelse](#).

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 [+47 40 03 50 31](tel:+4740035031)

Varsling av ikke tidskritiske hendelser:

E-post til incidents@helsecert.no

