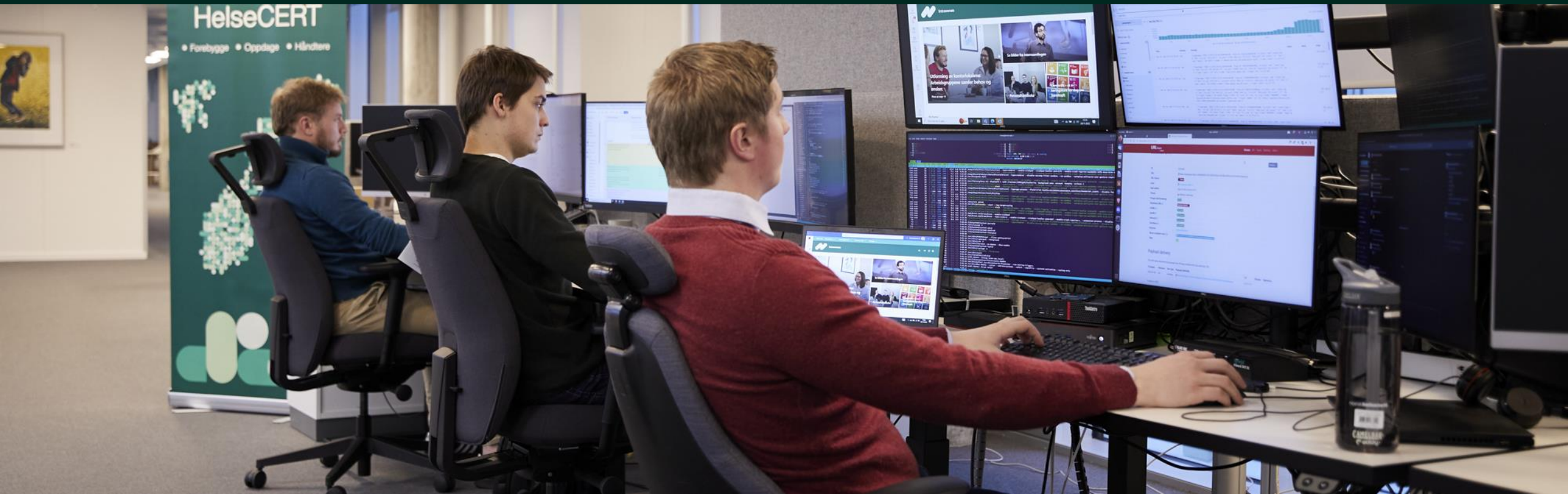
Norsk helsenett

Helse- og KommuneCERT Situasjonsbilde

KiNS-tech

Gunnar A. Johansen



Nasjonalt beskyttelsesprogram

- Kommunene får tilgang til Nasjonalt beskyttelsesprogram (NBP)
- Formål med NBP:
  - Forebygge, oppdage og håndtere cyberangrep
  - Gjør helse- og kommunesektoren så sikker som mulig
  - Utvikle og tilby tjenester som gir verdi for sektoren

Sikkerhetsutfordringer

- Nasjonal sikkerhet – et felles ansvar
- Krevende trusselbilde
- Utfordrer vår motstandsdyktighet
- Virksomheter trenger råd og veiledning

Situasjonsbilde

Trussel fra organiserte kriminelle

Ransomware

- Ransomware forblir den største trusselen mot tilgjengelighet og konfidensialitet
- Flere hendelser mot helse- og kommunesektor internasjonalt så langt i år
  - Change Healthcare (AlphV / BlackCat)
  - NHS Dumfries og Galloway (Skottland) (INC Ransom)
- Statistikk viser oss at under ransomwareangrep øker dødelighetsraten ved sykehus i USA

Phishing

- Mye AiTM-phishing
- Varierende grad av sofistikasjon
- Finnes også kampanjer hvor geoblokkering ikke er effektiv

Anatomy of an AitM phish; Hvordan gjør de det?

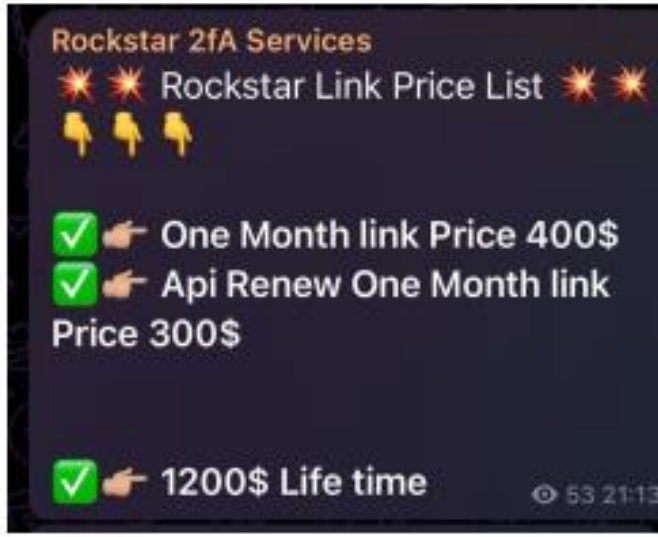
- Siden multifaktorautentisering (MFA) har blitt mye mer utbredt og krever nye teknikker for å omgås, har det oppstått et marked for kjøp og salg av verktøy for dette. Dette kalles AitM phishing.
- For tiden sporer vi mellom fem og ti ulike verktøy eller tjenester for AitM phishing.
- Noen slike verktøy 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.



Svindel

- Vi ser fortsatt sporadiske drypp av direktørsvindler
  - Mye kjøp av gavekort
- Fakturasvindelaktøren vi har fulgt siden 2019 har sporadisk vært aktiv i Norge de siste årene
  - Ikke kjent med gjennomførte svindler fra aktøren i perioden
  - Tidligere sett svindelforsøk på opptil 17 millioner norske kroner

Trusselen fra hacktivister

- Lite aktivitet fra hacktivister mot våre sektorer så langt i år.
- Fokus til hacktivistgrupper endrer seg raskt
  - Betente mediesaker
  - Skiftende geopolitisk situasjonsbilde
- Klar sammenheng mellom mediesaker og hacktivisters prioriteringer
- Noen angrep mot Norge siste tiden
- Forventer at statlige aktører gjemmer seg bak hacktivist-merket

Trussel fra statlige aktører

- Kapasiteten og kompetansen til statlige aktører øker kraftig
- Flere hendelser så langt i år mot kritisk infrastruktur
  - Volt Typhoon
    - Statlig kinesisk kampanje for å posisjonere seg med kontroll over store deler kritisk infrastruktur
  - Antatt IRGC-koblet aktør kompromitterte vannverk i USA
  - Vi forventer at statlige aktører jobber for å oppnå tilsvarende tilganger i norsk kritisk infrastruktur
- Vi er ikke kjent med angrep fra statlige aktører mot våre sektorer så langt i år

Sårbarheter

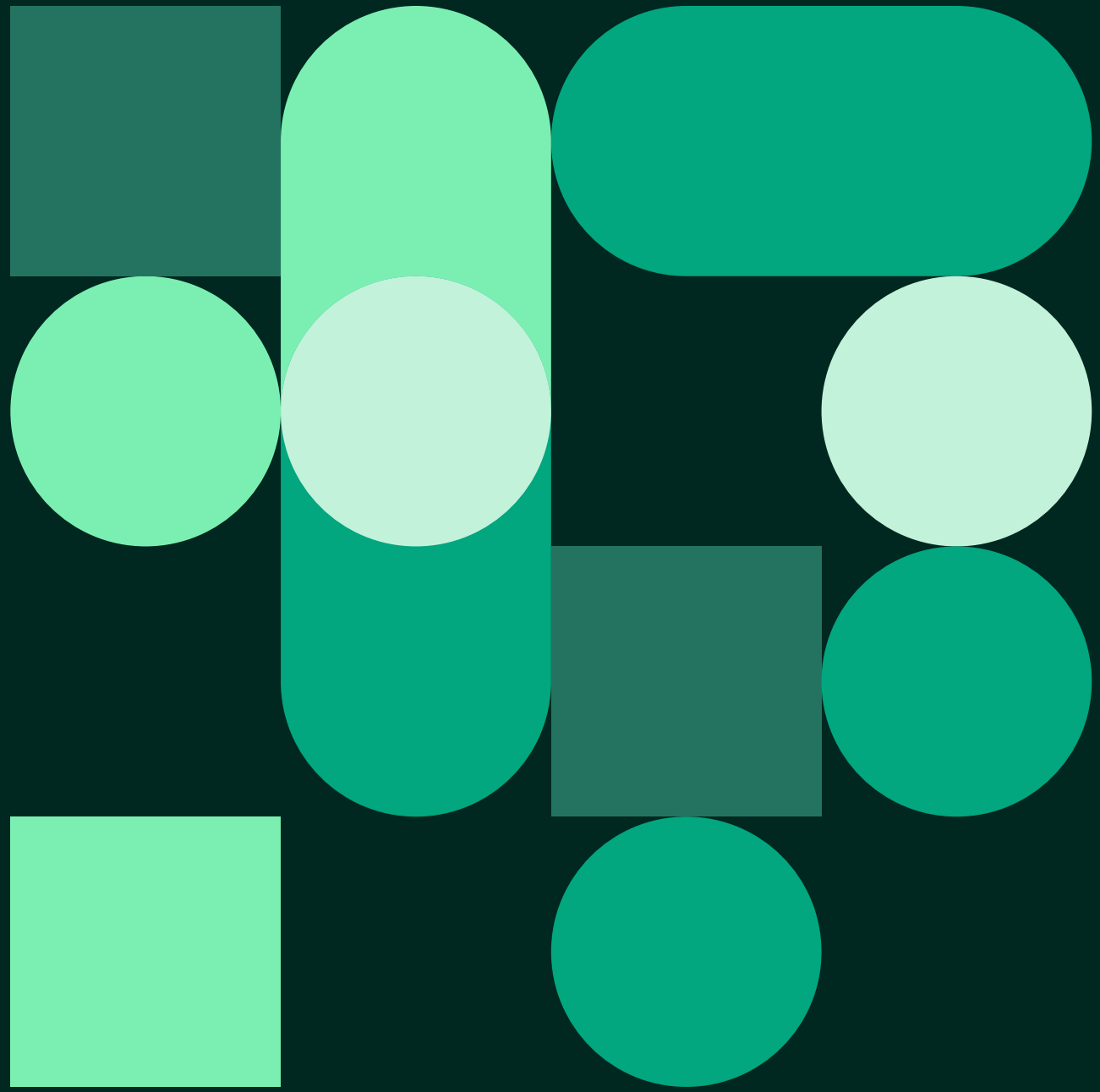
- Kritiske sårbarheter i internetteksponerte tjenester
- VPN-mottak har vært utsatt
- Oppdater systemer jevnlig
- Masseutnyttelse av sårbarheter etter kort tid

Hendelser siste tiden

- Ingen store enkelthendelser
- Jobbet med flere sakskompleks
  - Propagerende M365-phishing der MFA også phishes (AiTM)
  - Misbruk av varemerker i helsesektoren i phishingkampanjer
    - Ser bruk av "bulletproof" hosting i de aktuelle kampanjene
    - Spesielt Proton66 (AS198953) og Prospero (AS200593)
- Mye sårbarheter i internetteksponert utstyr
  - Fortinet, Citrix, Ivanti ConnectWise
- Ser for mange admingrensesnitt på internett

Norsk helsenett

Lov om digital sikkerhet



Lov om digital sikkerhet - Status

- Loven er vedtatt men ikke tredt i kraft
- Loven forutsetter at det utarbeides en forskrift før ikrafttredelse.
- Forslag til forskrift er ute på høring. Høringsfrist 11.desember
- § 24 i forskriften – «Ikraftredelse» lyder som følger:
  - Forskriften trer i kraft straks.

Lov om digital sikkerhet – hvem blir berørt

- Helse og omsorgstjenester som tilbys av en kommune med
  - Flere enn 50.000 innbyggere, eller
  - Flere en 20.0000 brukere av tjenesten, og
  - Tjenesten ikke kan avlastes av andre tjenester
- Vannforsyningssystemer som behandler minst 2000m3 pr døgn

- NIS2 utvider virkeområdet.
  - Offentlig forvaltning – sentral og regional
  - Avløpsvann

Lov om digital sikkerhet (digitalsikkerhetsloven) - krav

- § 6. Styringssystem for sikkerhet
- § 7. Risikovurdering
- § 8. Risikohåndtering
- § 9-11. Organisatoriske, teknologiske og fysiske sikkerhetstiltak
- § 13. Hendelseshåndtering og beredskap

- § 17 Varslingsplikt innen 24 timer

Vaksinasjon – tiltak og forebyggende aktivitet

HVORDAN ØKE VÅR MOTSTANDSDYKTIGHET?

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, men som kan redusere risiko vesentlig sammenliknet med å ikke ha det.
  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.

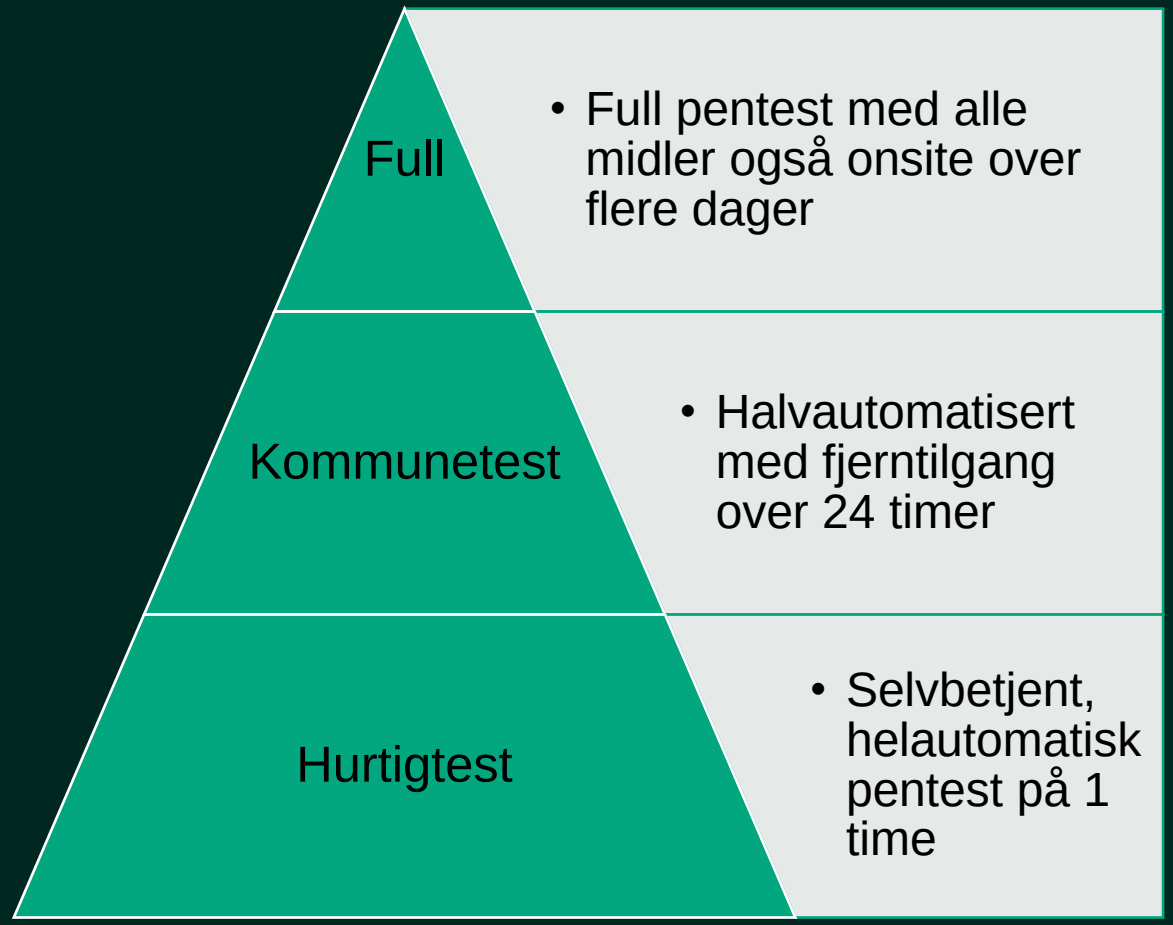
- **OBS**: Bruk av passord + multifaktorautentisering er sårbart for phishing og er derfor ikke godt nok. Slike angrep er beskrevet i eget webinar.
    - Se også vårt webinar om phishingresistent autentisering

HelseCERT | KommuneCERT - vi gjør helse- og kommunesektoren sikrere.

Hurtigtest for cybersikkerhet

- Automatisert sikkerhetstest
- Kjøres av hvert enkelt medlem
- Ser etter kjente svakheter fra inntrengingstester
- Ting som er relativt enkle å utbedre

Våre inntrengingstester



Norsk helsenett

Helse- og KommuneCERT

Gunnar A. Johansen

post@helsecert.no

helsecert.no