Universitetet i Oslo

CMMI for cybersikkerhetsstyring

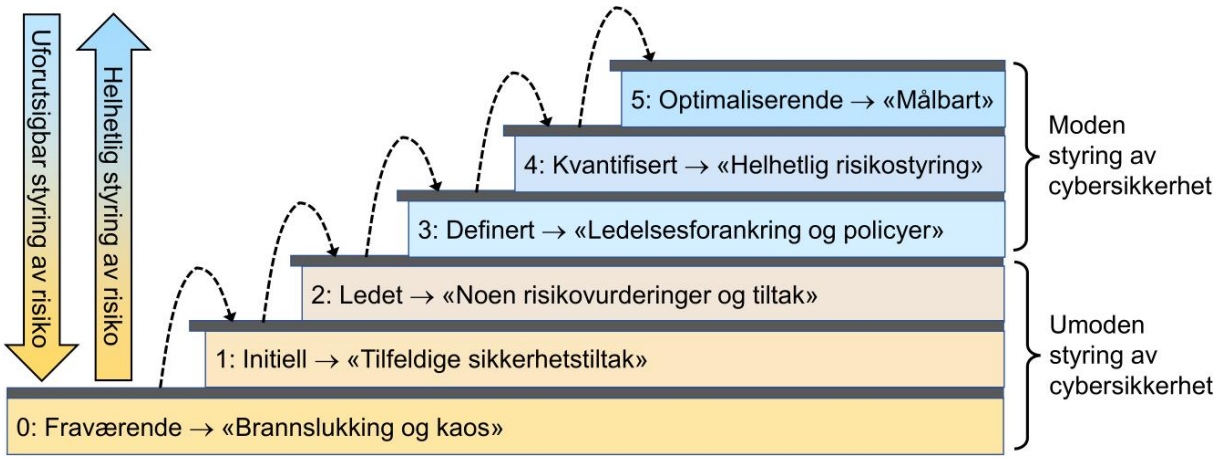
UiO, 2025

Bakgrunn

Capability Maturity Model Integration (CMMI) er en prosessforbedringsmodell først utviklet i 1999 ved Software Engineering Institute (SEI) ved Carnegie Mellon University (CMU). På den tiden hadde man ofte svært umodne prosesser for programvareutvikling som resulterte i programvare med dårlig kvalitet, derav motivasjonen for en prosessforbedringsmodell. CMMI ble etter hvert utvidet til å omfatte andre prosesser enn bare programvareutvikling, og brukes i dag bl.a. til å vurdere og forbedre modenhet av prosesser relatert til cybersikkerhet i virksomheter. CMMI definerer modenhet på en skala fra 1 til 5. CMMI-modellen og tilhørende verktøy publiseres nå av CMMI Institute som er en del av ISACA[1]. CMMI har eksistert i forskjellige versjoner gjennom årene. Den nyeste er versjon 3.0 som ble publisert i 2023. CMMI kan benyttes for å vurdere nåværende modenhet i forhold til ønsket modenhet for cybersikkerhet i en virksomhet, og er dermed et verktøy for å begrunne nødvendige investeringer i cybersikkerhet. Med CMMI vurderes modenhet på et overordnet nivå. En lignende modenhetsmodell er NIST CSF Tiers[2] (Cybersecurity Framework) som beskriver fire modenhetsnivåer. For å vurdere cybersikkerhetsmodenhet på et mer teknisk nivå ut ifra hvilke sikkerhetstiltak som er implementert, kan man benytte Finans Norge sitt verktøy for vurdering av modenhet i beskyttelse mot, og respons på, cyberangrep[3]. Dette verktøyet er basert på sikkerhetstiltakene som er beskrevet i NSMs Grunnprinsipper for IKT-sikkerhet[4].

CMMI for cybersikkerhet

Figuren nedenfor viser modenhetsnivå 1 – 5 definert i CMMI, samt nivå 0 som egentlig ikke er definert som et modenhetsnivå, men som kan være relevant.



Modenhetsnivåer i CMMI for cybersikkerhet, versjon 3.0 (2023).

[1] https://cmmiinstitute.com
[2] https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf
[3] https://www.forsikringsdrift.no/cybersikkerhet/
[4] https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnprinsipper-for-ikt-sikkerhet/

De ulike nivåene i CMMI for cybersikkerhet er kort beskrevet nedenfor.

Nivå 0: Fraværende
En virksomhet uten noen oppmerksomhet på cybersikkerhet har fraværende modenhet. Ingen sikkerhetstiltak er implementert annet enn standard konfigureringer på PC-er og applikasjoner. Virksomheten er antagelig helt uforberedt om en sikkerhetshendelse skulle inntreffe.

Nivå 1: Initiell
En virksomhet der noen ansatte kan ha en viss oppmerksomhet på cybersikkerhet har initiell modenhet. Enkelte sikkerhetstiltak kan være implementert tilfeldig eller ut ifra intuisjon av noen som utfører IT-relaterte oppgaver. Imidlertid mangler kvalitetskontroll, konsistens og oppfølging av sikkerhetstiltak.

Virksomheten opptrer reaktivt ved sikkerhetshendelser, noe som betyr at den har dårlig eller manglende skrevne prosedyrer for hendelser med dertil uforutsigbare utfall. Virksomheten kan ha ansatte med noe sikkerhetsekspertise, men med begrenset kunnskap om strategi eller taktikk for å håndtere trusler effektivt.

Nivå 2: Ledet
En virksomhet der en mellomleder, men ikke en toppleder, har oppmerksomhet på cybersikkerhet har ledet modenhet. Virksomheter på dette nivået har fortsatt en reaktiv holdning, men gjennomfører visse prosjekter relatert til cybersikkerhet basert på presserende behov, kanskje ut ifra risikovurderinger. Prosesser rund sikkerhet forblir udokumenterte.

Nivå 3: Definert
En virksomhet med en overordnet policy der informasjons- eller cybersikkerhet er definert som en målsetting har definert modenhet. Nivå 3 er et stort sprang fra nivå 2 ved at cybersikkerhet har ledelsesforankring gjennom den overordnede policyen. Sikkerhetsprosjekter og prosessene følger til en viss grad anerkjente standarder for sikkerhets- og risikostyring. Virksomheten er typisk proaktiv i sin tilnærming til sikkerhetshendelser ved å ha en viss grad av cyberberedskap.

Nivå 4: Kvantifisert.
En virksomhet med helhetlig sikkerhets- og risikostyring har kvantifisert modenhet. Det betyr også at sikkerhetsprosjekter, -prosesser og -tiltak er målbare etter definerte metrikker. Dette modenhetsnivået krever et erfarent sikkerhetsteam med sterkt lederskap, budsjett og støtte fra toppledelsen.

Nivå 5: Optimaliserende.
En virksomhet som allerede har helhetlig sikkerhets- og risikostyring, og som i tillegg samler metrikker og KPI-er for cybersikkerhet har optimaliserende modenhet. Metrikker og KPI-er gjør at virksomheten kan optimalisere bruk av ressurser og investeringer i cybersikkerhet. Metrikkene bidrar også til mer objektive estimater for sannsynlighet og konsekvens ved risikovurderinger, noe som gjør risikovurderingene mer pålitelige som grunnlag for investeringer i sikkerhetstiltak.