CRA-KLARHETSSJEKK / EKSEMPEL

Fra spredte sikkerhetsnotater til en konkret evidensplan.

Fiktiv pilotrapport for Northstar Edge Gateway NX-4 - et oppdiktet produkt laget for å vise format, prioritering og detaljnivå.

PILOTPRIS

1 990 kr inkl. mva. - betaling etter levering

VIKTIG

Dette er et fiktivt eksempel, ikke en vurdering av en virkelig virksomhet eller et produkt. Leveransen er ikke juridisk rådgivning, sertifisering eller garanti for CRA-samsvar.

01 / SAMMENDRAG

Hva denne sjekken gjør

Sjekken oversetter tilgjengelig produktinformasjon til et arbeidskart: hvilke bevis som finnes, hvilke som ikke er observert, hvem som bør eie neste steg, og hva som kan ferdigstilles på 30 dager.

5	30	0
Evidensgap	**Dagers plan**	**Kildekode**
Tre bør prioriteres før rapporteringsplikten starter.	Tiltak med eier, bevis og ferdigkriterium.	Piloten krever ikke tilgang til kildekode.

Fiktiv produktprofil

Felt	Eksempelgrunnlag
Produkt	Northstar Edge Gateway NX-4
Funksjon	Industriell IoT-gateway med firmware, webadministrasjon, mobil installasjonsapp og valgfri skytjeneste.
Distribusjon	Selges til bedriftskunder i EU/EØS gjennom distributør og direkte salg.
Materiale brukt	Fiktiv produktside, hurtigstartguide, utgivelsesnotater og supportside.
Ikke brukt	Kildekode, kundedata, sårbarhetsdetaljer eller penetrasjonstest.

Foreløpig retning

Eksempelmaterialet gir ikke nok synlig evidens til å forklare sikkerhetsansvar gjennom hele produktets levetid. Første prioritet er å samle eksisterende praksis i godkjente, versjonerte bevis.

02 / DOKUMENTASJONSGAP

Fem gap som blir til arbeid

'Ikke observert' betyr bare at beviset ikke finnes i det avtalte grunnlaget. Det er ikke en konklusjon om at arbeidet aldri er gjort.

ID	Prioritet	Ikke observert	Hvorfor det betyr noe	Neste bevis
G-01	Høy	Versjonert produktrisiko	Sikkerhetsvalg og rest-risiko kan ikke spores til produktet.	Godkjent risikoregister.
G-02	Høy	Sårbarhetsprosess	Varsling, triage og frister kan bli personavhengige.	Prosedyre med 24/72-timers beslutningspunkt.
G-03	Høy	Komponentoversikt	Konsekvensanalyse for sårbarheter blir treg.	SBOM/register med eier.
G-04	Middels	Publisert støtteperiode	Kunder og team mangler ett felles svar.	Godkjent støttebeslutning.
G-05	Middels	Release-bevis	Tester, avvik og godkjenning er ikke samlet per utgivelse.	Sikker release-sjekkliste.

TOLKNING Siden prioriterer dokumentasjon og sporbarhet. Den vurderer ikke teknisk sikkerhetsnivå eller formell produktklassifisering.

03 / EVIDENSSJEKKLISTE

Hva teamet bør finne igjen

Hvert punkt bør ha en navngitt eier, versjon eller dato, godkjenningsstatus og en stabil lenke.

Område	Minimumsbevis	Eksempelstatus	Eier
Produkt	Omfang, markeder, grensesnitt og avhengigheter	Delvis	Produkt
Risiko	Versjonert risikovurdering og akseptert rest-risiko	Ikke observert	Produkt + sikkerhet
Komponenter	SBOM/register, versjon, leverandør, lisens og sårbarhetskobling	Ikke observert	Utvikling
Sårbarheter	Kontakt, mottak, triage, eskalering, retting og publisering	Ikke observert	Sikkerhet + support
Releaser	Krav, testbevis, kjente avvik, godkjenning og distribusjon	Delvis	Engineering
Oppdateringer	Signering, distribusjon, tilbakeføring og kundevarsling	Åpent spørsmål	Engineering/ops
Støtteperiode	Fastsettelse, publisering, endringsstyring og sluttdato	Ikke observert	Ledelse/produkt
Hendelser	Loggkilder, alvorlighetskriterier, beslutningsspor og øvelse	Ikke observert	Sikkerhet/ledelse
Brukerinfo	Sikker installasjon, oppdatering, kontakt og avvikling	Delvis	Produkt/support

Ferdigkriterium

Et punkt er først klart når dokumentet finnes, har eier og versjon, er godkjent, og kan knyttes til det konkrete produktet eller releasen.

04 / 30-DAGERS PLAN

Lukk det viktigste først

Planen er laget for et lite produktteam. Den starter med eierskap og minimumsbevis, deretter øves rapporteringsflyten.

Når	Tiltak	Ansvar	Ferdig når
Dag 1-3	Bekreft produktgrense, markeder, aktive versjoner og eiere.	Ledelse + produkt	Én godkjent omfangsside.
Dag 4-8	Opprett komponentregister for aktiv firmware-release.	Utviklingsleder	Versjon, leverandør, lisens, eier og kilde.
Dag 9-13	Dokumenter mottak, triage, eskalering og beslutningslogg.	Sikkerhet	Godkjent prosedyre og saksmal.
Dag 14-18	Lag første produktrisikovurdering.	Produkt + sikkerhet	Versjonert risiko og rest-risiko.
Dag 19-22	Fastsett støtteperiode og sikkerhetskontakt.	Ledelse + produkt	Publisert og godkjent.
Dag 23-26	Bygg sikkerhetsdelen av release-sjekklisten.	Engineering	Test, avvik, sign-off og kundemelding.
Dag 27-30	Kjør øvelse på en fiktiv aktivt utnyttet sårbarhet.	Sikkerhet + ledelse	Tidslinje, beslutningslogg og varslingsutkast.

RESULTAT ETTER 30 DAGER Ett produktomfang, navngitte eiere, grunnbevis for komponenter og risiko, og en øvd hendelsesflyt. Videre arbeid blir målbart.

05 / ÅPNE SPØRSMÅL

Det som må avklares videre

01	Hvilken juridisk enhet plasserer produktet på EU-markedet?
02	Hvilke programvare- og skytjenester er nødvendige for funksjonen?
03	Hvordan oppdages, prioriteres, signeres og distribueres oppdateringer?
04	Hvilke aktive versjoner og kundekonfigurasjoner må støttes?
05	Hvilke tester, revisjoner og sertifiseringer kan gjenbrukes som evidens?

Metode og avgrensning

Sjekken sammenligner avtalt grunnmateriale med en praktisk evidensmodell for produkt, komponenter, releaser, sårbarheter, hendelser, støtteperiode og brukerinformasjon. Den tester ikke produktet og erstatter ikke juridisk eller teknisk spesialrådgivning.

Offisielle referanser

Kilde	Lenke
EU Cyber Resilience Act	digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act
Rapporteringsplikter	digital-strategy.ec.europa.eu/en/policies/cra-reporting
Kommisjonens CRA-veiledning, 27. juli 2026	digital-strategy.ec.europa.eu/en/library/commission-publishes-new-guidance-timely-cyber-resilience-act-implementation
Forordning (EU) 2024/2847	eur-lex.europa.eu/eli/reg/2024/2847/oj

BESTILL EGEN SJEKK

1 990 kr inkl. mva. Betaling etter levering. projectleviathan1969@gmail.com. Ingen telefon, abonnement eller kildekodetilgang.