01 OMFATTNING

Noex

Omfattas din maskin av CRA?

Cyber Resilience Act gäller normalt produkter med **digitala element** vars avsedda ändamål eller rimligen förutsebara användning omfattar direkt eller indirekt dataanslutning.

1
STEG 1

Har produkten digitala element?

Det innebär att produkten innehåller programvara eller hårdvara med digital funktion.

Exempel

- PLC
- HMI
- Industri-PC
- Frekvensomriktare
- Säkerhetsstyrsystem
- Inbyggd programvara

JA

2
STEG 2

Har produkten dataanslutning?

Det innebär att produkten är direkt eller indirekt ansluten till en enhet eller ett nät.

Exempel

- Ethernet
- Profinet
- OPC UA
- USB
- WLAN
- Bluetooth
- Fjärrsupport

Typ av anslutning

Logisk anslutning
Via programvara eller nätverksprotokoll.

Fysisk anslutning
Via kabel, radiovågor eller annat fysiskt gränssnitt.

Indirekt anslutning
Via t.ex. fabriksnätverk, gateway eller molntjänst.

JA

CRA är normalt tillämplig när båda dessa kriterier är uppfyllda.

Även indirekt anslutning via exempelvis fabriksnätverk eller gateway kan omfattas.

3
STEG 3

Omfattas produkten av något undantag?

Vissa produktgrupper omfattas inte av CRA.

Exempel på undantag

- Medicintekniska produkter
- In vitro-diagnostik
- Vissa fordon
- Luftfartsprodukter
- Marina produkter m.fl.

NEJ

VIKTIGT: TA KONTROLL NU!

Produkten omfattas normalt av CRA.

- Utvecklingskrav
- Säkerhetskrav
- Vulnerability management

Påbörja arbetet med att säkerställa efterlevnad och planera för kontinuerlig säkerhet under hela produktens livscykel.

JA

Produkten omfattas inte av CRA.

Dokumentera bedömningen och spara underlag för spårbarhet.

Viktigt att tänka på

Bedömningen ska utgå från produktens avsedda ändamål och rimligen förutsebara användning. Vissa produktgrupper omfattas av annan sektorslagstiftning och kan därför vara undantagna från CRA.

Källa

CRA artikel 2 (tillämpningsområde) och artikel 3 (definitioner).

02 RAPPORTERINGSSKYLDIGHET • ARTIKEL 14 & 16

Noex

Rapporteringsskyldigheter från 11 september 2026

Från och med den 11 september 2026 måste tillverkare rapportera:

- **Aktivt utnyttjade sårbarheter**
- **Allvarliga incidenter** som påverkar säkerheten hos produkter med digitala element

RAPPORTERINGSTIDSLINJE

1. Tidig varning
≤ 24 timmar

Efter att tillverkaren fått kännedom om:
- en aktivt utnyttjad sårbarhet eller
- en allvarlig incident som påverkar produktens säkerhet

2. Formell anmälan
≤ 72 timmar

Information om:
- sårbarheten eller incidenten
- dess påverkan
- vidtagna eller planerade korrigerande åtgärder
- åtgärder som användaren kan vidta

3. Slutrapport
(aktivt utnyttjad sårbarhet)

14 dagar

Senast 14 dagar efter att korrigerande eller riskreducerande åtgärder blivit tillgängliga.

Rapporten ska bland annat innehålla:
- beskrivning av sårbarheten
- konsekvenser och allvarlighetsgrad
- information om säkerhetsuppdateringar eller andra korrigerande åtgärder

4. Slutrapport
(allvarlig incident)

1 månad

Senast en månad efter incidentanmälan.

Rapporten ska bland annat innehålla:
- detaljerad beskrivning av incidenten
- sannolik orsak eller hotkälla
- genomförda och pågående riskreducerande åtgärder

Gemensam rapporteringsplattform

Rapportering ska ske via **ENISA:s gemensamma rapporteringsplattform** enligt artikel 16.

Plattformen vidarebefordrar informationen till berörda CSIRT-enheter i de medlemsstater där produkten har tillhandahållits samt till andra behöriga myndigheter.

Berörda användare ska informeras

Tillverkaren ska underrätta berörda användare och, när det är lämpligt, samtliga användare om:
- sårbarheten eller incidenten
- möjliga konsekvenser
- riskreducerande åtgärder
- tillgängliga korrigerande åtgärder

Informationen ska, när så är lämpligt, tillhandahållas i ett **strukturerat och maskinläsbart format**.

Tidsfristerna räknas från den tidpunkt då tillverkaren får kännedom om händelsen. Rapporteringsskyldigheterna framgår av **artikel 14.** Rapporteringen sker via den gemensamma rapporteringsplattform som beskrivs i **artikel 16.**

Källa
Cyber Resilience Act (EU) 2024/2847, artikel 14 och 16

03 UTFORDRINGEN

Noex

Många komponenter – många potentiella sårbarheter

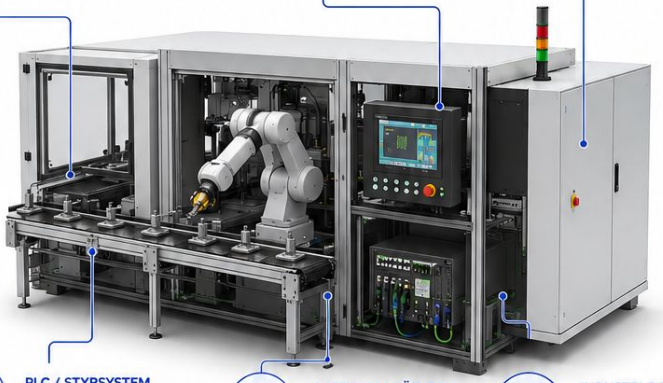
Ett modernt maskinsystem består ofta av flera produkter med digitala element. Varje komponent kan omfattas av egna cybersäkerhetsrisker, säkerhetsuppdateringar och rapporterade sårbarheter.

KOMPONENTER I ETT MASKINSYSTEM

SENSORER
Samlar in data från maskinens omgivning, processer och tillstånd.

HMI / OPERATÖRSPANEL
Gränssnitt för övervakning och interaktion mellan operatör och maskin.

DRIVSYSTEM
Frekvensomriktare, servodrifter och andra system som styr rörelse och kraft.



PLC / STYRSYSTEM
Programmerbar styrning som hanterar maskinens logik och funktioner.

GATEWAY / NÄTVERK
Ansluter olika komponenter och möjliggör kommunikation och dataöverföring.

INDUSTRI-PC
Kör applikationer, lagrar data och hanterar bearbetning lokalt i maskinen.

Varje komponent måste bedömas

När nya sårbarheter offentliggörs behöver tillverkaren avgöra:

- Om den berörda komponenten används i maskinen
- Om sårbarheten påverkar den egna produkten
- Om riskreducerande eller korrigerande åtgärder krävs
- Om rapporteringsskyldigheter enligt CRA kan aktualiseras

Manuell analys är tidskrävande

Att identifiera, bedöma och följa upp sårbarheter i flera digitala komponenter kan kräva betydande resurser – samtidigt som tidsfristerna på **24 och 72 timmar** måste uppfyllas.

Viktigt att tänka på

Tillverkaren ansvarar för att ha en strukturerad process och verktygsstöd för att kunna hantera sårbarheter i alla relevanta komponenter – i tid.

Källa
Cyber Resilience Act (EU) 2024/2847, artikel 14 och 16

04 LÖSNINGEN • CSAF

Noex

CSAF – strukturerad och maskinläsbar säkerhetsinformation

CSAF

CSAF (Common Security Advisory Framework) är en öppen standard för att publicera och utbyta säkerhetsinformation i ett strukturerat och maskinläsbart format. Standarden gör det möjligt att automatiskt behandla information om sårbarheter, berörda produkter och rekommenderade åtgärder från olika leverantörer.

1 Strukturerad information

Leverantören publicerar säkerhetsinformation om sårbarheter, berörda produkter och åtgärder i CSAF-format (JSON).

2 Maskinläsbart format

Informationen är strukturerad och maskinläsbar, vilket möjliggör automatisk tolkning utan manuell bearbetning.

3 Automatiserad behandling

System och verktyg kan automatiskt hämta in, filtrera och behandla informationen.

4 Identifiera berörda produkter

Det blir enkelt att identifiera vilka produkter, komponenter och versioner som påverkas.

5 Rekommenderade åtgärder

Rekommenderade åtgärder och rekommendationer kan kommuniceras och förstås entydigt av mottagande system.

Snabbare och mer effektiv sårbarhetshantering

Strukturerad och maskinläsbar information minskar manuell hantering, felrisken och tiden från publicering till åtgärd.

CSAF i korthet

Öppen standard
CSAF är en öppen standard som kan användas av alla.

OASIS-standard
Utvecklad och förvaltad inom OASIS Open.

ISO/IEC 20153
CSAF är godkänd som internationell standard ISO/IEC 20153.

Maskinläsbart format
Säkerhetsinformation publiceras i JSON-format för enkel maskinläsning och automatisering.

Nytta för din organisation

- Mindre manuell hantering och snabbare processer
- Minskad risk för fel och missförstånd
- Bättre interoperabilitet mellan system och organisationer
- Aktuell och korrekt information – vid rätt tidpunkt
- Stöd för automatisering och skalbar säkerhetshantering

Artikel 14.8 i CRA anger att sådan information, **när det är lämpligt**, ska tillhandahållas i ett format som är enkelt att automatiskt behandla.

Snabbare identifiering av berörda komponenter

När leverantörer publicerar CSAF-filer kan verktyg automatiskt identifiera vilka komponenter som berörs och stödja bedömningen av den egna produktens påverkan.

Det **minskar den manuella arbetsinsatsen** och underlättar arbetet med sårbarhetshantering.

Källa
Cyber Resilience Act (EU) 2024/2847, artikel 14.8

05 I PRAKTIKEN

Noex

CSAF gör säkerhetsinformation enklare att använda

När leverantörer publicerar säkerhetsmeddelanden i CSAF-format kan informationen behandlas automatiskt och integreras i organisationens processer för sårbarhetshantering.

Det gör det enklare att identifiera berörda produkter, bedöma påverkan och hantera säkerhetsinformation från flera leverantörer.

Så fungerar det i praktiken

1 Leverantör publicerar säkerhetsmeddelande i CSAF-format

Strukturerad information om sårbarheter, berörda produkter och åtgärder.

2 Informationen publiceras

Meddelandet görs tillgängligt via webbadress eller integrationskanal.

3 Automatisk bearbetning

System och verktyg hämtar, tolkar och validerar CSAF-data automatiskt.

4 Identifiering av berörda produkter

Berörda produkter, komponenter och versioner matchas mot din miljö.

5 Rekommenderade åtgärder

Rekommendationer och åtgärder presenteras och kan integreras i arbetsflöden.

CSAF-format – maskinläsbart

- Strukturerat JSON-format
- Designat för automatisk tolkning
- Enkel integration i verktyg och processer
- Stöd för exakt och konsekvent information

PDF-format – människoläsbart

- Avsett för manuell läsning
- Kräver manuell granskning och tolkning
- Svårare att integrera i system
- Risk för missad eller fördröjd information

Effektivare hantering av säkerhetsinformation

Maskinläsbar säkerhetsinformation minskar manuellt arbete och ger snabbare tillgång till relevant information om:

- Berörda produkter
- Identifierade sårbarheter
- Rekommenderade åtgärder

Fördelar med CSAF i praktiken

Snabbare respons

Automatiserad hantering ger kortare tid från publicering till åtgärd.

Högre träffsäkerhet

Exakt matchning mot produkter och versioner minskar risken för fel.

Enkel integration

Fungerar med befintliga verktyg och processer genom öppna standarder.

Skalbart

Hanterar stora mängder information och många leverantörer samtidigt.

Ökad säkerhet

Rätt information i rätt tid ger bättre beslutsunderlag och minskar risker.

Genom att använda CSAF-format kan organisationer skapa en mer automatiserad, pålitlig och skalbar process för hantering av säkerhetsinformation – oavsett antal leverantörer.

Källa

Cyber Resilience Act (EU) 2024/2847, artikel 14.8

06 FÅ KONTROLL ÖVER CRA-KRAVEN

Noex

Från krav till praktiskt arbete

För att uppfylla Cyber Resilience Act (CRA) behöver tillverkare ha kontroll över sina komponenter, cybersäkerhetsrisker, sårbarheter och säkerhetsuppdateringar **från utveckling till slutet av produktens stödperiod.**

Nedan visas sex centrala områden som hjälper dig att bygga en process för att uppfylla CRA:s krav i praktiken.

Viktigt att komma ihåg

CRA handlar inte enbart om rapportering. Tillverkare måste kunna identifiera komponenter, hantera sårbarheter, distribuera säkerhetsuppdateringar och informera användare **från utveckling till slutet av stödperioden.**

Läs mer i CRA

- Artikel 13 – Tillverkares skyldigheter
- Artikel 14 – Rapportering
- Bilaga I Del I – Krav på egenskaper
- Bilaga I Del II – Krav på sårbarhetshantering

Källa
Cyber Resilience Act (EU) 2024/2847