digitaliserings og ligestillingsministeriet

Sagsnr.
2023 - 1125

Doknr.
14953

Dato
20-04-2023

Opfølgning på teknisk gennemgang af Cyber Resilience Act den 12. april 2023

Eksempler på, hvad forordningen betyder for en almindelig lille virksomhed eller forening, der ikke er producent af produkter med digitale elementer

Forslaget gælder for virksomheder, der enten selv producerer produkter med digitale elementer og bringer dem på det indre marked, eller som gør det på vegne af en anden virksomhed – fx via import eller distribution.

Her skelnes der som udgangspunkt ikke mellem store og små virksomheder, men der er i forslaget åbnet for, at vurderingsorganer bør tage en virksomheds størrelse i betragtning, når de fastsætter prisen for udførelse af overensstemmelsesvurderinger og test.

For virksomheder, der ikke producerer eller bringer produkter på markedet i eget navn, etablerer forslaget ikke nogen forpligtelser. Der er altså ingen regler i forslaget om, at man som erhvervsdrivende – lille eller stor – holdes ansvarlig for cybersikkerheden i produkter man bruger.

Eksempel: *En lille virksomhed anvender som led i deres forretning bl.a. et tekstbehandlingsprogram, en computer og en kopimaskine. Pga. en sårbarhed i en eller flere af dem, bliver virksomheden hacket og følsomme informationer om deres kunder stjålet. Forslaget pålægger i denne situation ikke virksomheden noget ansvar, hverken i forhold til deres kunder eller medarbejdere eller for at rapportere det til myndighederne. Efter forslaget er det altså alene producenten eller dennes repræsentant, der kan blive holdt ansvarlig.*

Forpligtelser der følger af anden lovgivning, som fx om persondatabeskyttelse, arbejdsgiveransvar eller almindelig erstatningsret, gælder naturligvis stadig – det ændrer forslaget ikke ved.

Forslaget vil tværtimod stille virksomheder, der bruger produkter med digitale elementer bedre end før. Dels fordi cybersikkerhedsniveauet i produkter løftes, men også fordi producenterne i højere grad end før kan stilles til ansvar. Endelig vil både erhvervsdrivende og forbrugere også få bedre adgang til information om sikkerheden i produkterne og hvordan de anvendes på en sikker måde

Hvad er de økonomiske gevinster af forslaget i Danmark?

Det er svært at give et præcist tal på, hvad de økonomiske gevinster bliver i Danmark. Det skyldes, at forslaget stadig er under forhandling, hvorfor reglerne ikke ligger helt fast endnu, men også at der ikke findes mange undersøgelser på området.

Baseret på tal fra Danmarks Statistik og en rapport fra 2022 af SMV-Danmark, har Digitaliseringsstyrelsen estimeret – med betydelige usikkerheder – at den samlede årlige omkostning som følge af cybersikkerhedshændelser i Danmark er ca. 1,8 mia. kr., fordelt på godt 2.300 virksomheder.

En del af denne omkostning vil kunne undgås, når CRA implementeres. Der er dog også en del cyberangreb, fx phishing, hvor sårbarheden ligger hos brugeren selv og ikke i produktet. Sådanne angreb indgår i de samlede omkostninger, men vil ikke direkte blive påvirket af reglerne i CRA.

Endvidere sætter CRA alene krav om et minimumsniveau af cybersikkerhed, og vil derfor heller ikke forhindre de mere avancerede cyberangreb, der ofte fører til større omkostninger.

Endelig vil der også gå noget tid, før produkter, der allerede er taget i brug før forslaget finder anvendelse, og dermed ikke er omfattet af størstedelen af kravene, bliver helt udfaset. Disse kan derfor fortsat udgøre en risiko.

På denne baggrund er et konservativt skøn, at ca. en tredjedel af de nævnte angreb på sigt kunne undgås, hvilket svarer til en årlig besparelse på ca. 600 millioner kr. Besparelsen vil formentlig blive større med tiden, både i takt med at gamle produkter udfases, og fordi brugen af produkter med digitale elementer forventes at stige eksponentielt.

Her er der dog ikke taget højde for eventuelle afledte effekter, som fx et styrket fokus på cybersikkerhed hos brugerne når de anskaffer og anvender produkter, og at cybersikkerhed dermed også bliver en større konkurrenceparameter for virksomhederne.

Hvilken rolle spiller risikovurdering i forslaget?

Risikovurdering er et helt centralt element i forslaget, der skal sikre, at producenterne foretager en grundig gennemgang af deres produkt og processer, uden at blive pålagt urimelige krav, som ville gøre produkterne uforholdsmæssigt dyre.

Efter forslaget skal producenter foretage en vurdering af cybersikkerhedsrisiciene, før et produkt må gøres tilgængeligt på det indre marked. Resultatet skal tages i betragtning under planlægning, design, udvikling, produktion, levering og vedligeholdelse af produktet.

Det er på baggrund af denne vurdering, at overholdelse af forslagets 'væsentlige krav' til cybersikkerheden i produktet skal vurderes. Det betyder bl.a., at disse krav kan tilpasses det enkelte produkt og dets tilsigtede brug.

Forslaget sikrer på den måde en proportionel og balanceret tilgang, hvor virksomheder ikke forpligtes til at tage højde for alle mulige hensyn og sikkerhedsforanstaltninger, men alene dem, der er relevante og har en væsentlig betydning for sikkerheden i det enkelte produkt og den sammenhæng, det skal fungere i.

Risikovurderingen skal også indgå i den tekniske dokumentation, som producenten skal udarbejde og efter anmodning dele med tilsynsmyndighederne. På den måde står virksomhederne på mål for deres vurdering, og myndighederne tilsynsarbejde lettes.

Endelig er forpligtelsen til at foretage en sådan risikovurdering også en vigtig øvelse for producenterne, der kan tilføje dem nyttig viden om og øget fokus på cybersikkerhed. Det kan hjælpe dem til at opdage potentielle risici og sårbarheder i deres egne systemer og processer generelt.

Hvilke regler gælder for produkter og producenter uden for EU?

For at en producent kan gøre et produkt tilgængeligt på det indre marked, skal det pågældende produkt leve op til EU's regler, uanset af hvem og hvor det er produceret. Det vil altså sige, at lever et produkt ikke op til reglerne, så må det ikke sælges i Danmark eller andre EU-lande.

Dette er det samme princip, som gør sig gældende ved anden EU-produktsikkerhedslovgivning, og reglerne vil skulle håndhæves i overensstemmelse med markedsovervågningsforordningen.

Forpligtigelserne hviler som udgangspunkt på producenterne. Dog kan andre økonomiske aktører, såsom bemyndigede repræsentanter, importører og distributører, overtage visse af producentens forpligtelser, afhængigt af deres rolle og handlinger.

Bemyndigede repræsentanter kan udpeges af producenter, der ikke er etableret i EU, til at repræsentere dem over for markedsovervågningsmyndighederne. De skal sørge for, at producentens tekniske dokumentation er tilgængelig for markedsovervågningsmyndighederne, og samarbejde med dem, fx ved at informere dem om eventuelle risici ved producentens produkter.

Importører og distributører er ansvarlige for at sikre, at de produkter, de importerer fra lande uden for EU, overholder forslagets krav. De skal fx sørge for, at producenten har foretaget de nødvendige overensstemmelsesvurderinger og forsyne produkterne med de nødvendige oplysninger, som fx CE-mærkning samt deres og producentens navn og adresse.

I visse tilfælde overtager importører eller distributører helt producentens forpligtelser. Det sker fx hvis de bringer produktet i omsætning under eget navn, eller foretager væsentlige ændringer af et produkt, der allerede er bragt i omsætning.