Lov & Data er et nordisk tidsskrift for rettsinformatikk og utgis av

Lovdata
Postboks 6688 St. Olavs plass
NO-0129 Oslo, Norge
Tlf.: +47 23 11 83 00
E-post: lovogdata@lovdata.no
Nettside: www.lod.lovdata.no
Alias: www.lovogdata.no
www.lawanddata.no

Elektronisk: ISSN 1503-8289
Utkommer med 4 nummer pr. år.

Lov & Data er medlemsblad for foreningene Norsk forening for Jus og EDB, Dansk forening for Persondataret, Danske IT-advokater, Svenska föreningen för IT och juridik (SIJU) og Finnish IT Law Association.

Fra 2024 er Lov & Data kun tilgjengelig på nett, lod.lovdata.no.

Lov & Data

Layout: Aksell AS

Leder

Cybersikkerhed bliver produktsikkerhed

Tue Goldschmieding

EU's ambitioner om regulering af det digitale marked omsættes i disse år til konkret handling, og med introduktionen af ny lovgivning bevæger IT-retten sig for alvor fra anvendelse af generel lovgivning i det digitale rum til selvstændig regulering af den digitale verden, med fokus på de særlige problemstillinger, der udspringer af de digitale teknologier og øget brug af data. En af de seneste tilføjelser til denne regulatoriske bølge er Cyber Resilience Act. Cyber Resilience Act adskiller sig fra anden informations- og cybersikkerhedslovgivning som NIS2-direktivet ved at være egentlig produktsikkerhedslovgivning. Cyber Resilience Act opstiller således ikke alene krav til producentens tekniske foranstaltninger og efterlevelse af best practice, men opstiller krav til informations- og cybersikkerheden i produkter, der er bestemmende for producentens produktansvar og markedsadgang.

Cyber Resilience Act konkretiserer informations- og cybersikkerhedskravene. Når sårbarheder opdages, er håndteringen ikke længere alene et internt anliggende, men et krav med direkte betydning for salg, udbud, kontrakter og kundetillid. Sårbarhedsrapportering bliver et markedskrav frem for blot et potentielt kontraktkrav. For produkter med digitale elementer bliver forventningen, at leverandøren ikke bare kan håndtere sårbarheder, men skal have en systematisk proces for at modtage og behandle sårbarhedsrapporter, vurdere risiko og påvirkning, informere relevante myndigheder ved alvorlige forhold, informere kunder og brugere når det er nødvendigt og levere rettelser og opdateringer som en del af produktets livscyklus.

Ticket to play

Udsagn som »vi tager sikkerhed alvorligt« vil i fremtiden ikke længere være tilstrækkeligt. Informations- og cybersikkerhed i produkter er en

verificerbar størrelse, og troværdig sårbarhedshåndtering en konkurrenceparameter på linje med kvalitet og pris.

Udbud og indkøb vil i stigende grad stille ufravigelige krav til sikker produktudvikling, sårbarhedsprocesser, opdateringspolitik og dokumentation. Leverandører, der kan svare klart og konsistent, vil vinde. Samtidig vil kunder i stigende grad kræve klare kontraktlige forpligtelser om patching, responstider, advisering og transparens. Når et sikkerhedshul udnyttes, handler tvisten ofte ikke om, hvem der fandt fejlen, men om hvem der gjorde hvad, hvornår, og hvorvidt leverandøren kan dokumentere sin proces.

Tiden er knap

Cyber Resilience Act stiller krav til producentens håndtering af det digitale produkts cybersikkerhed gennem hele produktets livscyklus og forudsætter, at producenten har etableret den organisation og de interne processer, der er nødvendige for at håndtere de stillede krav.

På trods af at Cyber Resilience Act har indflydelse langt ind i producentens organisation og forretningsgange, er Cyber Resilience Act for mange producenter gået under radaren eller er blevet sat til side, mens producenten har forholdt sig til NIS2 eller den megen anden digitale lovgivning, der er blevet introduceret.

Det fulde sæt af forpligtelser under Cyber Resilience Act træder i kraft for digitale produkter, der bringes på markedet fra den 11. december 2027 og reglerne om rapportering af sårbarheder træder i kraft allerede den 11. september 2026.

Dette giver producenterne mindre end to år til at etablere de processer og funktioner, der er nødvendige for producentens overholdelse af de materielle krav under Cyber Resilience Act. Disse krav forudsætter, blandt andet, at producenten har implementeret processer til sikring af cybersikkerhed i design fasen, håndtering af cybersikkerhed i tredjepartskomponenter, udarbejdelse af dokumentation og håndtering af sårbarheder, og rapportering.

> Cyber Resilience Act adskiller sig fra anden informations- og cybersikkerhedslovgivning som NIS2-direktivet ved at være egentlig produktsikkerhedslovgivning.

For mange producenter vil denne tidsfrist være udfordrende henset til, den tid, det tager at udvikle nye digitale produkter og fordi implementeringen kræver omfattende organisatoriske og tekniske ændringer.

Mange producenter bør derfor allerede nu påbegynde implementeringen af de mange krav, der sikrer, at de nødvendige processer, dokumentation og organisatoriske kapaciteter er på plads inden ikrafttrædelsen.

Udfordringen i softwareforsyningskæden og rapporteringskrav

For producenter af digitale produkter er identifikation og håndtering af sårbarheder hidtil blevet foretaget efter bedste evne, når producenten blev opmærksom på en sårbarhed. Derfor har mange kontrakter alene opstillet krav om, at producenten skulle håndtere sårbarheder, som producenten måtte blive bekendt med. Cyber Resilience Act er et opgør med denne praksis. Producentens identifikation og håndtering af sårbarheder i produkters cybersikkerhed og informationssikkerhed er ikke længere blot et internt kvalitetsmål, men et lovgivningsmæssigt krav, som kunder, partnere og myndigheder kan måle producenten på, og er afgørende for producentens markedsadgang og konkurrenceposition.

I de fleste tilfælde opstår sårbarheder ikke i den kode, producenten selv har udviklet, men i de tredjepartskomponenter, der anvendes i produktudviklingen. Cyber Resilience Act stiller derfor også krav til, at producenten har styr på sin softwareforsyningskæde. Grundlæggende skal producenter have afdækket og forstået, hvilke softwarekomponenter, der indgår i producentens produkter (Software Bill of Materials) og skal have implementeret processer, der sikrer, at producenten kan identificere og adressere sårbarheder i disse komponenter.

Cyber Resilience Act opstiller også krav til producentens deling af oplysninger om sårbarheder og rapportering af sårbarheder, der har været udnyttet. Producenter skal derfor agere efter en præmis om transparens for både kunder og myndigheder i producentens håndtering af sårbarheder og den potentielle ansvarseksponering, der kan opstå, hvis producenten ikke håndterer sårbarheder korrekt.

Producentens identifikation og håndtering af sårbarheder i digitale produkter bliver således ikke blot en compliance-øvelse, men en multidisciplinær proces, der kræver forståelse af både regulatoriske krav, tekniske forhold, kommunikation og kontraktuelle forpligtelser og rettigheder i forholdet til kunder og leverandører.

Tue Goldschmieding, partner i Gorrissen Federspiel og dansk redaktør for Lov & Data.