In deze rubriek geven enkele IB-redacteuren in een kort stukje hun reactie op recente nieuwsitems over informatiebeveiliging. Dit zijn persoonlijke reacties van de auteurs en deze geven niet noodzakelijkerwijs het officiële standpunt weer van hun werkgever of van PvIB. Vragen en/of opmerkingen kun je sturen naar ibmagazine@pvib.nl.

Cyber Resilience Act: tijd voor verantwoorde softwarekwaliteit

Het onderwerp van AHN in dit nieuwe jaar valt voor velen van u naar alle waarschijnlijkheid in de categorie 'klein nieuws'. Voor mij persoonlijk (Leo van Koppen) is het groot nieuws! Al zo'n twintig jaar verbaas ik me over, nee sterker nog, kijk ik met afschuw naar de wijze waarop softwareproducenten omgaan met hun verantwoordelijkheid. Hét nieuws van deze week gaat daar, naar ik hoop en ook wel verwacht, eindelijk verandering in brengen. De Cyber Resilience Act (CRA), die op 11 december 2024 van kracht is geworden, markeert een mijlpaal in softwareverantwoordelijkheid binnen de EU. Eindelijk gaan er eisen gesteld worden aan software, apps, hardware, IoT en digitale producten.

De wet is al aangekondigd in najaar 2022 en het heeft al twee jaar geduurd voordat er enige overeenstemming is gevonden in de uiteindelijke uitvoering. Met de stapsgewijze intrede hebben producenten de tijd om aan de eisen te gaan voldoen, ze hebben de tijd om de wettelijke eisen te vertalen naar de wijziging/invoering van de interne processen. Belangrijke data zijn: 11-12-2024 inwerkingtreding, 11-12-2026 meldplicht in werking, 11-12-2027 wetgeving volledig van kracht.

Belangrijkste elementen in de wetgeving:

1. In de ontwerp- en ontwikkelingsfase dienen security-eisen te worden meegenomen
2. Beperking van het aantal aanvalsoppervlakken zoals interfaces
3. Een risicobeoordeling dient onderdeel te zijn van het ontwikkelproces en dient opgenomen te worden in de technische documentatie
4. Aflevering van de producten in een veilige standaard configuratie


Fook Hwa Tan


Leo van Koppen

Het moment om samen de schouders eronder te zetten en een betrouwbaar digitaal landschap te creëren

5. Producten moeten een conformiteitsprocedure ondergaan en met een CE-markering aantonen te voldoen aan de security eisen
6. Er dient een periode gedefinieerd te worden waarin beveiligingsupdates worden verstrekt
7. Melding van actief misbruikte kwetsbaarheden
8. Importeurs en distribiteurs moeten ervoor zorgen dat producten aan de security eisen voldoen als ze op de Europese markt komen

Ik verwacht dat de wet de nodige impact zal hebben voor producenten en leveranciers, met name bij de implementatie in hun ontwikkelprocessen, de meldplicht en de update-garantietijd. Overtredingen kunnen leiden tot boetes van maximaal 15 miljoen euro of 2,5% van de jaarlijkse wereldwijde omzet, afhankelijk van wat hoger is.

Hoewel dit voor sommige producenten een uitdaging zal zijn, biedt de CRA ook een kans om vertrouwen op te bouwen bij klanten en concurrentievoordeel te behalen. Een déjà vu naar de invoering van de GDPR? Ik ben niet alleen geïnteresseerd wat de redacteuren ervan vinden, maar ben eigenlijk nog meer benieuwd wat u als lezer hiervan vindt.

Fook Hwa Tan – Kwaliteit in een nieuw tijdperk: hoe de Cyber Resilience Act hoop biedt voor softwareontwikkeling

De invoering van de Cyber Resilience Act (CRA) is een doorbraak. Het is niet zomaar een stap, maar een mijlpaal op weg naar een digitaal Europa dat veiliger, transparanter en verantwoordelijker is. Voor sommigen misschien klein nieuws, maar voor wie het belang van kwaliteit begrijpt, is dit groot – revolutionair zelfs. Neemt niet weg, dat onze eindbestemming bereiken nog wel wat tijd gaat kosten.

Eindelijk wordt de technologie-industrie tot actie gemaand De CRA gaat verder dan het opleggen van regels; het vraagt om een fundamentele cultuurverandering. Het dwingt ons de vraag te stellen: wat betekent het om verantwoordelijkheid te nemen voor de digitale producten die ons leven doordringen? Hoe zorgen we ervoor dat kwaliteit en veiligheid geen losse eindjes zijn, maar vanaf de eerste schets tot de laatste update stevig verankerd zijn in elke fase van ontwikkeling?

En dit is nog maar het begin. De CRA omarmt een holistische aanpak die verder reikt dan softwarekwaliteit alleen. Het pakt de kern van digitale veiligheid aan door:

- Beveiliging te eisen vanaf de ontwerpfase (Security by Design) en veilige standaardconfiguraties te verplichten
- Interfaces en aanvalsoppervlakken te beperken, waardoor cyberaanvallen minder kans krijgen
- Risicobeoordelingen en technische documentatie te verplichten – geen vage beloftes meer, maar harde, toetsbare feiten
- Fabrikanten te dwingen beveiligingsupdates te garanderen en kwetsbaarheden te melden, om vertrouwen en transparantie te bevorderen
- Importeurs en distributeurs medeverantwoordelijk te maken voor naleving, waardoor de hele keten scherp blijft

Ja, de CRA vraagt veel. Het zal bedrijven dwingen om hun processen opnieuw uit te vinden. Het betekent werk. Het betekent verandering. Maar laten we eerlijk zijn: is dat niet precies wat nodig is? Is het niet tijd dat we stoppen met het accepteren van halve oplossingen en ons richten op echte vooruitgang?

De CRA is niet alleen een verplichting, maar ook een kans. Een kans om te excelleren. Een kans om vertrouwen te winnen. Een kans om technologie echt in dienst te stellen van mensen, zonder ze bloot te stellen aan onnodige risico's.

Het is een belofte. Een belofte van een digitale toekomst waarin veiligheid de norm is, waarin kwaliteit geen optie is, maar een fundamenteel recht. Dit is het moment om samen de schouders eronder te zetten en een digitaal landschap te creëren waar we allemaal op kunnen vertrouwen. Wat denkt u? Sluit u aan en help ons de lat hoger te leggen. De tijd van half werk is voorbij – samen bouwen we aan een veilige, rechtvaardige digitale wereld.