Aandachtspunten bij uitvoeringswet CRA

(Wet tot uitvoering van Verordening (EU) 2024/2847)

Memorie van toelichting 2.(b). Paragraaf 2 op pagina 6 “Software Bill of Materials (SBOM)”

Fabrikanten zijn verplicht op hun website de product of lifecycle te vermelden. Hoewel goed omschreven in de wetteksten van de CRA zullen fabrikanten dat allemaal op hun eigen manier gaan invullen. Dat leidt tot diversiteit en staat heldere transparantie in de weg.

Wat heel goed zou zijn is het aanleggen van een centraal register, beheerd door de toezichthouder of, beter, door Enisa, waarin alle fabrikanten die digitale producten aan de Europese markt (gaan) leveren hun producten moeten registreren. Mocht registratie op Europees niveau niet mogelijk zijn, stel dan een nationale registratie in, bijvoorbeeld via de in de memorie van toelichting genoemde SBOM.

Overweeg deze gegevens daarin op te nemen / toe te voegen:

1. Merknaam
2. Type aanduiding en omschrijving
3. Type product (router, switch, firewall, deur sensor, lift sensor, etc)
4. Product dat bij falen kan leiden tot menselijk leed (Ja/Nee)*
5. EAN code
6. EOL / EOS datum
7. Productpagina waar de update link staat

Daarnaast zou het fijn zijn dat een API gefaciliteerd te worden die tegen deze database kan praten. Toegang reguleren via (gratis) registratie en acceptatie. Dat kan op termijn, zodra marktpartijen hierop inspelen, snel (geautomatiseerd) vaststellen of een kwetsbaarheid van toepassing is faciliteren.

* De NIS 2 uitvoeringsverordening (EU) 2024/2690 artikel 3.1.(c) hanteert als één van de criteria voor het classificeren van een incident als een significant incident: Kan het incident fatale gezondheidsschade aan het individu veroorzaken? “the incident has caused or is capable of causing the death of a natural person”. In de CRA en diens uitvoeringsverordening wordt vaker verwezen naar de NIS 2 (EU) 2022/2555, waarbij de CRA uitvoering van de NIS 2 effectiever kan maken. Zeker als het om (mogelijke) incidenten die menselijk leed kunnen veroorzaken gaat is snel handelen een belangrijke factor. Als alle producten een kenmerk hebben dat mogelijk menselijk leed kwalificeert kan, als voor zo’n product een kwetsbaarheid signalering uitgaat, hier een bijzondere aandacht voor worden gegeven. Dat maakt snel en adequaat handelen mogelijk en voorkomt wellicht (fatale) schade aan het individu.

Memorie van toelichting 3.(a):

Wat te doen als de distributeur aan de fabrikant vraagt haar CE keurmerk / digitaal keurmerk voor het product te delen [art 20.2(b) CRA] maar de fabrikant weigert. Is er een arbitrage mogelijkheid via de toezichthouder RDI? Of is het simpelweg: Dan wordt dat product niet door de distributeur geleverd en de bestaande leveringen teruggehaald. Wie draait op voor de kosten? Wat als een eindklant weigert het product te retourneren? Welke partij(en) plegen dan inbreuk op de CRA? Is de distributeur in dat geval gevrijwaard (vanwege tussen partij en voldaan aan zorgplicht naar eindklant)?

Memorie van toelichting 4. Derde paragraaf:

Blijft het bestaande CE logo / keurmerk gehandhaafd en komt er een nieuw waaruit blijkt dat het product voldoet aan de nieuwe eisen, CRA gebaseerd [bijlage 1 artikel 2 CRA]?

Wat te doen met de bestaande installed base? Die zal lang niet altijd voldoen aan de CRA-eisen zoals het niet kunnen aanpassen van het wachtwoord, er komen geen updates uit, etc. Je kunt als maatregel die devices in een netwerksegment zetten en daarmee isoleren. Is daarmee voldaan de CRA voldaan? [bijlage 1, artikel 2(i) CRA] “de negatieve impact van de producten zelf of van verbonden apparaten op de beschikbaarheid van diensten die door andere apparaten of netwerken worden geleverd, tot een minimum beperken;”

Wat doen we met oude software die geen robuust gebruikersbeheer ondersteund of geen SSL-verbindingen kent? Of geen updates ondersteund? Kan die achter een applicatie proxy worden gezet om daarmee secure te worden? [bijlage 1, artikel 2(i) CRA]