© Blue Planet Studio / Adobe Stock

Verbonden apparaten en cyberbeveiliging: de EU onderneemt actie!

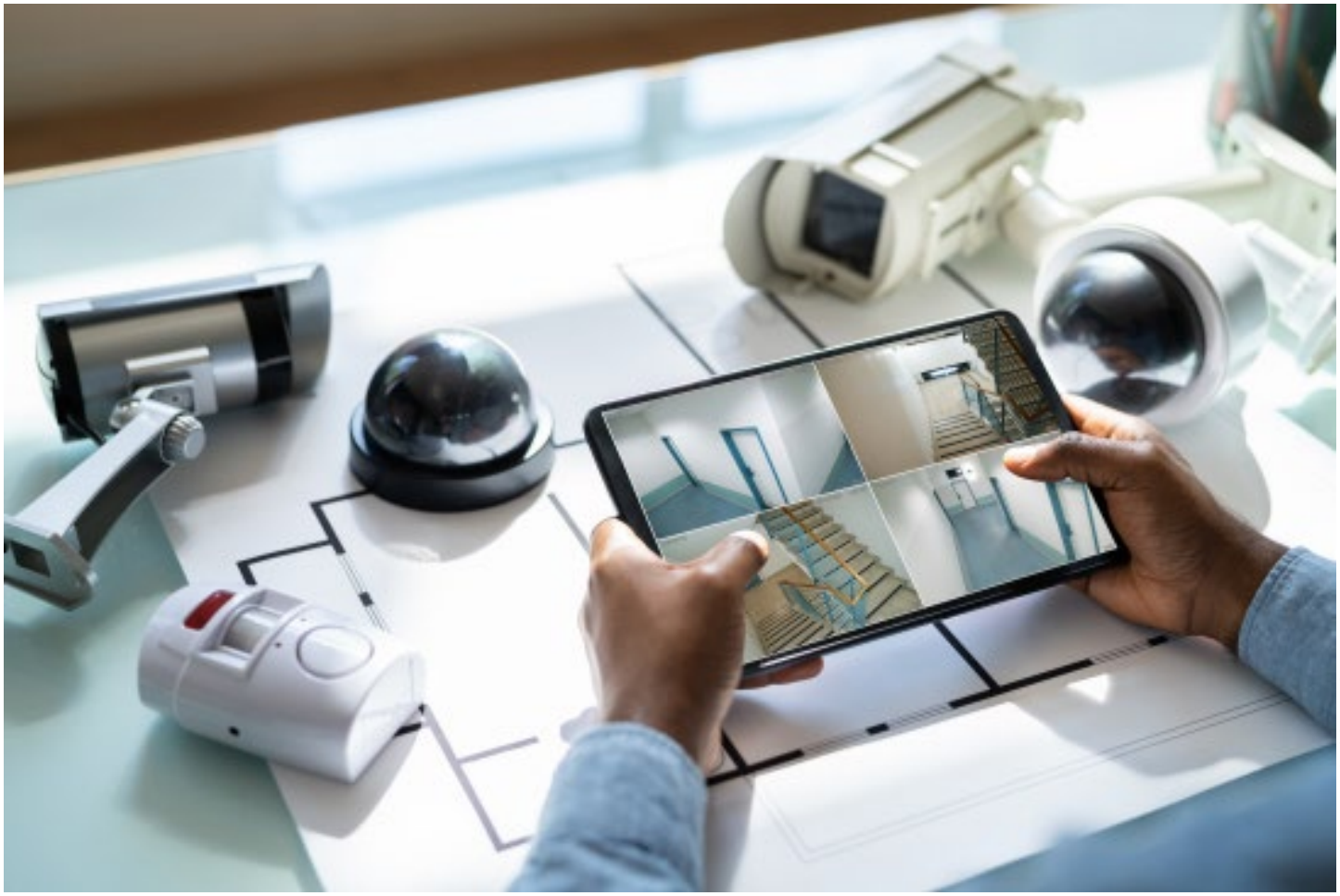
Alle mogelijke apparaten onbeveiligd toegang geven maakt de netwerken kwetsbaar, vooral als die apparaten niet gemachtigd zijn. Omgekeerd dreigen die verbonden apparaten "overgenomen" te worden door die ongemachtigde netwerken en het doelwit te worden van aanvallen of frauduleuze handelingen. Om dit te verhelpen zijn betrouwbare, schaalbare automatische mechanismen nodig om de verbonden apparaten gedurende hun levenscyclus te beheren. Met de toekomstige "Cyber Resilience Act" wil de Europese Unie hier een antwoord op bieden[1].

We moeten de waarheid onder ogen zien. Heel wat verbonden of slimme producten hebben een bijzonder zwak beveiligingsniveau. ANPI houdt u regelmatig op de hoogte van deze situatie[2]. Bovendien brengen een aantal producenten geen updates uit om de kwetsbaarheden van hun producten te verhelpen. Die kwetsbaarheden brengen kosten mee wanneer de beveiliging faalt, zowel voor de consument als voor de professionele gebruiker. Die gebruikers beschikken vaak niet over voldoende nauwkeurige informatie bij de keuze van "veilige producten" en de vraag of ze op een veilige manier zijn geconfigureerd. Het algemeen basisprincipe dat vooropstaat in de Europese regelgeving is dat alleen "veilige" producten in de lidstaten op de markt mogen worden gebracht[3].

1 *Wetgeving omtrent cyberweerbaarheid (zie referentie aan het einde van het artikel).*

2 *Wanneer verbonden objecten onbruikbaar worden / Jeanine Driessens - Fire & Security Alert Magazine nr. 18, maart 2020, p. 79 ; Bewakingscamera's niet helemaal veilig / Fire & Security Alert Magazine nr. 16, september 2019, p. 52-53.*

3 *Veilig product: "een product dat bij normale of redelijkerwijs te verwachten gebruiksomstandigheden, ook wat gebruiksduur en eventueel indienststelling, installatie en onderhoudseisen betreft, geen enkel risico oplevert, dan wel slechts beperkte risico's die verenigbaar zijn met het gebruik van het product en vanuit het oogpunt van een hoog beschermingsniveau voor de gezondheid en de veiligheid van personen, aanvaardbaar worden geacht. […]" (Wetboek van economisch recht, art. I.10).*



© Andrey Popov / Adobe Stock

In het domein van cyberbeveiliging komt dit erop neer dat het product onder meer:

- als het zodanig is ontworpen en vervaardigd dat het een beveiligingsniveau heeft dat is afgestemd op de cyberrisico's die aan het gebruik ervan zijn verbonden;
- op het tijdstip van de verkoop geen bekende kwetsbaarheden vertoont;
- een standaardconfiguratie voor veilig gebruik heeft;
- tegen onrechtmatige verbindingen is beschermd;
- de gegevens die het verzamelt beschermt en
- alleen gegevens verzamelt die voor de werking ervan noodzakelijk zijn.

VOORSTEL VAN EUROPESE VERORDENING

De actualiteit toont dagelijks aan dat het van essentieel belang is om enerzijds effectiever te reageren op cyberaanvallen, en anderzijds cyberbeveiliging op Europees niveau te harmoniseren. En vervolgens ook op lidstaatniveau.

De Europese Commissie diende daarom een voorstel in voor verordening voor cyberweerbaarheid in ("Cyber Resilience Act" - CRA)[4] met strengere cyberbeveiligingsnormen om:

- een betrouwbaar systeem voor de marktdeelnemers tot stand te brengen en
- te garanderen dat de EU-burgers veilig gebruik kunnen maken van producten die op de markt zijn.

Dit cyberweerbaarheidsvoorstel heeft betrekking op vrijwel alle digitale producten (producten met digitale elementen en software), met uitzondering van producten van medische aard of producten die verband houden met de burgerluchtvaart, voertuigen en producten voor militaire doeleinden.

VIER DOELSTELLINGEN

Deze wetgeving beoogt vier doelen:

- ervoor zorgen dat fabrikanten de beveiliging van producten met digitale elementen in de ontwerp- en ontwikkelingsfase en gedurende de gehele levenscyclus ervan verbeteren;
- zorgen voor een samenhangend kader van voorschriften inzake cyberbeveiliging, zodat de naleving ervan voor fabrikanten gemakkelijker wordt;
- de transparantie van de beveiligingskenmerken van producten met digitale elementen verbeteren; en tenslotte
- bedrijven en consumenten in staat stellen om deze producten op een veilige manier te gebruiken.

4 *Zie referentie aan het einde van het artikel.*

Met het voorstel wordt in feite een CE-markering voor cyberbeveiliging geïntroduceerd die op alle onder de CRA vallende producten moet worden aangebracht.

BETROKKEN PRODUCTEN

Zoals hierboven aangegeven is de definitie van *"producten met digitale elementen"* erg ruim en omvat deze elk software- of hardwareproduct, alsook software of hardware die niet in het product is ingebouwd, maar afzonderlijk op de markt wordt gebracht.

Met de verordening worden verplichte vereisten inzake cyberbeveiliging ingevoerd voor producten met digitale componenten die de hele levenscyclus ervan bestrijken, maar ze komt niet in de plaats van de reeds bestaande vereisten. Reeds gecertificeerde producten die in overeenstemming zijn met al bestaande EU-normen zullen in het kader van de nieuwe verordening als "goedgekeurd" worden beschouwd.

De cyberweerbaarheidsverordening voorziet een "standaardcategorie" van producten en software. Deze kan worden vertrouwd op een zelfbeoordeling door de fabrikant, zoals reeds het geval is voor andere soorten CE-markering. Volgens de Commissie valt 90 % van de producten op de markt onder deze categorie. De producten in kwestie kunnen in de handel worden gebracht na een zelfbeoordeling van hun cyberveiligheid door de fabrikant die de in de richtlijnen voor de toepassing van de regels vermelde passende documentatie indient.

De overige 10 % van de producten wordt onderverdeeld in twee andere categorieën:

- klasse I voor "de minst gevaarlijke producten";
- klasse II voor "de gevaarlijkste producten" waarvan het in de handel brengen waakzaamheid vereist.

Het gaat om *"kritieke producten met digitale elementen"* waarvan het falen kan leiden tot andere gevaarlijke en bredere inbreuken op de beveiliging (de betrokken productcategorieën zijn opgenomen in een lijst in een bijlage bij het voorstel).

Voor producten in deze twee categorieën is de basiszelfbeoordeling alleen toegestaan als de fabrikant aantoont dat hij heeft voldaan aan specifieke marktnormen en beveiligingsspecificaties of aan reeds door de EU vastgestelde certificeringsregelingen voor cyberbeveiliging. Als dit niet het geval is, kan het product worden gecertificeerd door een geaccrediteerde certificeringsinstantie waarvan het attest verplicht is voor producten van klasse II.

CERTIFICERING, MARKTTOEZICHT EN SANCTIES

Strenge normen spelen een essentiële rol in de invoering en opzet van een robuust EU-cyberbeveiligingssysteem voor alle marktdeelnemers. Dat systeem zal consumenten de garantie geven dat ze elk product dat op de markt wordt gebracht in alle veiligheid kunnen gebruiken en zal hun vertrouwen in de digitale wereld vergroten.

Importhandelaars en verdelers zullen verplicht worden om de conformiteit van de fabrikant met de relevante procedures en de CE-markering van het product te controleren. De fabrikanten van kritieke producten van klassen I en II zullen een specifieke conformiteitsprocedure moeten volgen. Voor de apparaten van klasse II is een expertise door een derde partij vereist (certificeringsinstelling).

De bevoegde nationale autoriteiten zullen een lijst van vereisten moeten volgen om organen in te stellen die de evaluaties door derden verzekeren en markttoezichtsinstanties moeten instellen (bijvoorbeeld de cyberbeveiligingsautoriteiten). Zij zouden "bezemoperaties" kunnen houden, gelijktijdige en gecoördineerde controles van

© Bro Vector / Adobe Stock

© ryanking999/Adobe Stock

bepaalde producten om hun conformiteit na te gaan. In geval van non-conformiteit zullen de nationale autoriteiten het product op de Europese markt kunnen verbieden. Er zal ook een sanctieregeling worden voorzien.

EEN COMPROMIS?

Zoals elke wetgeving in ontwikkeling zal dit voorstel van verordening voorwerp zijn van wijzigingen en amendementen. Zo werd onlangs een compromis voorgelegd door Zweden dat momenteel het roterende voorzitterschap van de Raad van de EU waarneemt.

De bijlage die de productcategorieën opsomt zou vervangen kunnen worden door criteria. Het eerste criterium zou kunnen nagaan of het product beschikt over *"een functionaliteit gekoppeld aan cyberbeveiliging en in het bijzonder of deze hoofdzakelijk voor beveiliging essentiële functies vervult, met name de beveiliging van authenticatie en toegang, preventie en detectie van indringers, de beveiliging van terminals of de beveiliging van netwerken"*.

Het tweede criterium zou kunnen nagaan of het product een centrale systeemfunctie heeft, zoals het beheer van het netwerk, controle van de configuratie, virtualisatie, de verwerking van persoonlijke gegevens of iedere andere functie die de werking van verschillende verbonden apparaten kan verstoren.

Er worden ook aanvullende essentiële vereisten ingevoerd (unieke productidentificatie, verwijderen van gegevens en parameters van het product voor veilige verwijdering, cyberbeveiligingsrisicoanalyse op basis van voorziene functie en redelijk te verwachten gebruik, alsook specifieke gebruiksvoorwaarden).

Men zal uiteraard ook toekomstige ontwikkelingen nauw in de gaten moeten houden: vertrouwen in door slimme producten gebruikte technologieën vergroten is een heuse uitdaging ...

Christopher BOON
ANPI - Information, Marketing & Communication

Referentie: *Voorstel voor een verordening van het Europees Parlement en de Raad betreffende horizontale cyberbeveiligingsvereisten voor producten met digitale elementen en tot wijziging van Verordening (EU) 2019/1020 [COM(2022) 454]*

OM DE WETTELIJKE ONTWIKKELING TE VOLGEN:

- *Cyber Resilience Act - Procedure 2022/0272 (COD) https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2022/0272(COD)&l=nl*

TE RAADPLEGEN:

- *Position Paper on proposed Cyber Resilience Act / Euralarm, 20 January 2023 https://www.euralarm.org/resource/euralarm-releases-position-paper-on-cyber-resilience-act.html*
- *Zweeds voorzitterschap van de Raad van de EU stelt eerste volledige herziening van de cyberbeveiligingsverordening voor / Luca Bertuzzi - EURACTIV.com, 26 avril 2023 https://www.euractiv.fr/section/economie/news/la-presidence-suedoise-du-conseil-de-lue-presente-la-premiere-revision-complete-de-la-legislation-sur-la-cyberresilience/*