Auteurs: Chris de Vries is redacteur van iB-Magazine en werkt als consultant onder de naam De Vries Impuls Management. Chris is bereikbaar via impuls@euronet.nl. Mr. A.IJ. Ard Ruiter is bestuurslid van PvIB en werkt als privacy- en beveiligingsfunctionaris/senior inspecteur bij de ILT Inlichtingen en Opsporingsdienst (ILTIOD). Ard is bereikbaar via LinkedIn.

INTERVIEW

Drs. Johan van den Bosch MCM CISA (agentschap Telecom) projectleider CSA en NCCA:

‘Securitycertificering steeds meer een Europese aangelegenheid’

Sinds april van dit jaar heeft het Agentschap Telecom er een nieuwe taak bij: de Nationale Cybersecuritycertificeringsautoriteit (NCCA). Een interessant onderwerp waar we meer van willen weten. Johan van den Bosch, projectleider NCCA bij het AT, stond ons welwillend en geëngageerd te woord.

In onze samenleving is de beschikbaarheid en betrouwbaarheid van de digitale infrastructuur enorm belangrijk. Agentschap Telecom (AT) voert de wet- en regelgeving uit op dit gebied en houdt er toezicht op dat iedereen zich aan de regels, eisen en voorwaarden houdt. Het AT is een overheidsorganisatie en is ondergebracht bij het ministerie van Economische Zaken en Klimaat (EZK) en heeft zowel uitvoerende als toezichthoudende taken voor de digitale infrastructuur. Het agentschap doet dat ook op andere terreinen, zoals bijvoorbeeld de wet die toeziet op veilig graven (Wibon), weegschalen, goud, zilver of platina en ruimtevaartactiviteiten. De taken van het AT omvatten het werkgebied Nederland, waaronder ook Caribisch Nederland. Daarnaast doet het AT onderzoek en brengt ze trends op het gebied van technologie, media en digitale infrastructuur in beeld. De AT is de Nationale Cybersecuritycertificeringsautoriteit (NCCA) voor Nederland geworden.

Het AT gaat als NCCA de certificerings- en toezichtstaken uit CSA uitvoeren. Wat kunnen we verstaan onder de certificerings- en toezichtstaken uit CSA? Wat gaat u precies doen en wat merken we daarvan?
Van den Bosch: "De Wet beveiliging netwerk- en informatiebeveiliging (Wbni) is op 9 november 2018 ingevoerd. De Wbni volgt op de NIS-directive (in het Nederlands NIB-richtlijn) van de Europese Unie, die moet zorgen voor meer eenheid in beleid over netwerk- en informatiebeveiliging. Dit is de Nederlandse implementatie van de Directive on security of Network and Information Systems (NIS-directive). De Wbni dicteert onder meer dat organisaties passende technische en organisatorische maatregelen op het gebied van cybersecurity moeten nemen. Op de NIS komt een opvolger: NIS2. NIS2 moet de cybersecurity-eisen in Europa verhogen en meer organisaties aanmerken als essentieel bedrijf. Het gaat om zo'n 160.000 organisaties door heel Europa. Deze bedrijven moeten gaan voldoen aan hogere eisen."

Met enthousiasme vertelt Johan van den Bosch over de vier taken van de NCCA: "Twee taken gaan over de voorafgaande goedkeuring; de andere twee over het behoud en de handhaving van goede certificering. De eerste betreft de CSA-taak. Certificering gebeurt dan volgens de CSA-zekerheidsniveaus, te weten: 'basis', 'substantieel' en 'hoog risico'. Dat laatste, meest intensieve niveau, gaat om producten of diensten die een grotere impact op de samenleving hebben als het misgaat. Nederland kiest uitdrukkelijk voor het systeem van 'prior approval'. De certificering van de producten op het CSA niveau 'hoog' worden door NCCA voorafgaand aan de uitreiking van het certificaat extra gecontroleerd en goedgekeurd. Pas daarna mag door de certificerende instelling het certificaat aan haar klant, die een product of dienst heeft laten certificeren, worden uitgegeven. In Duitsland, Frankrijk, Italië en Spanje geeft de overheid zelf certificaten uit om diezelfde mate van controle te bereiken. De kracht van ons land: er zijn goede Nederlandse partijen in de markt voor conformiteitsbeoordeling. In Europa is Nederland één van de meest actieve landen en wij zijn één van de leidende inbrengers binnen het Europese samenwerkingsverband."

Waar staat CSA voor?
CSA staat voor Cyber Security Act, de Europese wetgeving voor cyberbeveiliging die sinds 2019 van kracht is en aansluit op de Wbni. Europese lidstaten hebben de laatste jaren, ieder voor zich, verschillende certificeringsverplichtingen ingevoerd. De CSA moet zorgen voor regels die voor alle lidstaten hetzelfde zijn. Fabrikanten en dienstverleners behalen straks niet meer in elk lidstaat afzonderlijk een certificaat. De Europese regeling vervangt dus vergelijkbare nationale certificeringen.

"De tweede taak van de NCCA heeft betrekking op de toelating van CBI's (Conformiteitsbeoordelingsinstanties) (1) tot het Europese certificeringsstelsel. De CBI's moeten CSA geaccrediteerd zijn gebaseerd op de ISO17065-norm. Dat is de ISO-norm die de vereisten vaststelt voor organisaties die producten, processen en/of diensten mogen certificeren. Deze vereisten omvatten de competentienormen vanuit de opgestelde certificeringsschema's. De NCCA toetst of CB's en CAB's voldoen aan de additionele eisen in het certificeringsschema (dus eisen bovenop de ISO17065). Monitoring van certificeringstrajecten op het CSA Assurance Level Hoog betekent dat bij een positief oordeel, een goedkeuring verleend wordt aan de CB voor uitreiking van het certificaat aan de klant van de CB die een product of dienst heeft laten certificeren.

In het geval van additionele eisen is dan verificatie nodig, zonder additionele eisen is enkel certificatie vereist. Is het niveau substantieel, dan zorgen Notified Bodies (NB) voor productcertificering. Dit gaat als proces verder omdat er hogere eisen worden gesteld dan bij de competentienormen. Die eisen zijn transparanter – want opgenomen in schema's –, in vergelijking met product-NB's. Certificatieclaims (QR-codes) worden gepubliceerd en zijn dus te controleren door de gebruiker (2)."

De derde taak van het NCCA is het toezicht dat achteraf plaatsvindt. Projectleider Van den Bosch vertelt dat het ook gaat om het controleren of gecertificeerde producten en diensten nog steeds voldoen aan de vereisten uit het certificeringsschema. "De eerste stap is dan controle van het certificatiedossier van de certificerende instelling. De tweede stap kan dan zijn verdere controles of hertesten van product of dienst bij de fabrikant of provider, de houder van het certificaat. Dit gebeurt zowel gedurende de levenscyclus van het product, de dienst en het proces als de geldigheidsduur van het certificaat. Opgave voor de fabrikant en dienstverlener zal het proces 'vulnerability handling' zijn: 'hoe behandel ik de kwetsbaarheden?' Kwetsbaarheden kunnen zich immers ook voordoen als het gecertificeerde product al in de markt is. Het resultaat van een certificatie in het verleden, is niet per se een garantie voor de toekomst. Dat proces kan leiden tot de noodzaak van hercertificatie, ook bij wijzigingen van of in het product. Uitgangspunt is dat er veel meer beheersing wordt gevraagd met betrekking tot de kwetsbaarheden, risico's en/of wijzigingen. Dit stelt dus specifiek eisen aan het management, de ontwikkeling, de productie en het beheer van IT-producten, -diensten en -processen."

Certificering in Europa

Wil een certificerende instelling (Certification Body (CB)) actief zijn onder een Europees CSA-schema, dan moet het door de Raad voor Accreditatie worden geaccrediteerd per CSA-certificeringsschema. Het eerste certificeringsschema zal zijn de 'Common Criteria based European Union Cybersecurity Certification scheme (EUCC)'. Dat schema vervangt het SOG-IS (basisschema in verschillende landen). Het EUCC-schema is bedoeld voor certificering van IT-producten, ook wel beveiligingsproducten genoemd. ENISA heeft het kandidaatschema opgeleverd aan de Europese commissie die de tekst verwerkt in een Europese regeling onder de CSA. Na de publicatie van de regeling zal Nederland de deelname aan het Nederlands Schema voor de Certificatie op het gebied van IT-Beveiliging (NSCIB) gaan beëindigen.

Wens EU om te harmoniseren

De EU wil harmoniseren, hetgeen een direct gevolg is van de Digital Single Market Strategy (DSMS). Het Europese Common Criteria certificeringsschema (EUCC) bevordert harmonisatie van nationale - met internationale normen en is een multilaterale overeenkomst onder deelnemende landen en certificatie-instanties. Meer dan 50 landen nemen momenteel deel aan de regeling, met inbegrip van de belangrijkste, industriële naties. Een tweede reden voor de wens om te harmoniseren is de verhoging van de cyberweerbaarheid, de digitale autonomie en datasoevereiniteit. Het wordt ook telkenmale in de Europese State of the Union geplaatst.

De vierde taak van het NCCA omvat het toezicht op CBI's en testlaboratoria. Dat toezicht bestaat uit: toetsing van de naleving door de CB van de verplichtingen die opgenomen zijn in de CSA- en EU- certificeringsschema's en de toetsing van de competenties van de CB. Passen zij certificeringseisen uit de EU certificeringsschema's op een juiste wijze toe? Johan van den Bosch beoordeelt of een Conformiteitsbeoordelingsinstantie Europese CSA-certificeringen kan en mag uitvoeren (toelating). Verder beoordeelt hij op het CSA-zekerheidsniveau 'hoog' of een CBI aan het einde van het certificeringstraject een Europees certificaat mag uitreiken (voorafgaande goedkeuring) en ten slotte of een geaccrediteerde CBI toestemming mag geven aan de fabrikant om het Common Criteria Recognition Arrangement-logo (CCRA) te gebruiken bij communicatie over een gecertificeerd product. Wat toezicht betreft, let het NCCA op de naleving van de certificeringsvereisten door fabrikanten en aanbieders die een IT-product, - dienst of –proces hebben laten certificeren alsook op de naleving van de certificeringsvereisten door de toegelaten CBI's.

Welk advies zou het Agentschap Telecom/de NCCA de lezers van iB-Magazine geven ten aanzien van scholing en uw certificatiebeleid?

Van den Bosch: "Na- of bijscholing is niet aan het NCCA. Het is verstandig dat leveranciers, afnemers en adviseurs de ontwikkelingen volgen en dan onder meer aandacht hebben voor de schema's die in ontwikkeling zijn en verplichtingen tot certificering die mogelijk in de nabije toekomst gaan gelden. Voor de lezer zal wel van belang zijn, de vraag: 'Wat betekent certificatie voor onze marktbenadering? Welke wensen kunnen klanten met betrekking tot die eisen naar voren brengen?' Uiteindelijk kunnen klanten bij de inkoop van producten en/of diensten CSA-certificeringen gaan eisen dan wel een voorkeur voor uitspreken. Onder de NIS2 zullen in Nederland circa 5.000 partijen vallen. Ook voor kleine bedrijven kan NIS2 spelen. Ga zo nodig – inzake de certificering – ook in gesprek met AT. Wacht niet totdat NIS2 actief wordt, dan ben je te laat! Cybersecurity wordt steeds meer een EU aangelegenheid, kijk dus naar de EU-ontwikkelingen en regelgeving. Let daarbij op de Data resilience act dat omvat alle data veiligheidseisen gekoppeld aan alle IT-producten."

Moeten onze lezers een kennis- en vaardigheidscertificaat bij de AT/NCCA binnenhalen?

"Kennis en vaardigheden over het thema certificering en marktsegmentatie (bijvoorbeeld inzake 'main archetypes suppliers/competitive dynamics IoT-market' (3)) zullen nodig zijn om een relatie tussen een schema en producten en diensten te kunnen leggen. Scholing is geen kerntaak van de NCCA, het advies is om de ontwikkelingen op de voet te volgen, zodat bedrijven er goed en tijdig op in kunnen spelen."

Ziet u hier knelpunten, zijn er voldoende gekwalificeerde CBI's en leeft de NIS-directive voldoende bij uw doelgroepen?

"Nederland heeft een sterke markt voor conformiteitsbeoordeling. Agentschap Telecom doet wat in haar vermogen ligt om bij de doelgroepen van regelgeving onder de aandacht te brengen. In het kader van de CSA is de doelgroep fabrikanten en providers lastig te benaderen, omdat deze groep heel groot is en zich over de hele wereld kan bevinden. Voor certificerende instellingen en testlaboratoria ligt dat anders, de groep die in Nederland actief is kennen we en daar zitten we al twee jaar mee om tafel. Het gaat in hier om IT-producten, -diensten en -processen."

Wat denkt u als u de zeer krappe, professionele markt in ogenschouw neemt en bedrijven een NCCA-certificaat willen behalen?

"Groot aandachtspunt. Ook het Agentschap Telecom zoekt mensen, en zeker bij de operationalisering van de eerste schema's met name dus vanaf het einde van dit jaar en 2023 en verder. Bel ons dus gerust. Het werk moet je natuurlijk wel liggen, het gaat om monitoren en toezichthouden; dat is werk met een grote maatschappelijke impact. Om- en bijscholing is wellicht een oplossing voor tekorten. Efficiënte combinaties van werk kunnen bijdragen daar waar het toezicht op de CSA en het toezicht op andere AT-toezichtsdomeinen elkaar raken."

"Effectiviteit aan het voorgaande is daarbij essentieel. Het AT streeft ernaar om haar toezichtstaken in samenhang op te pakken. Dit vanuit de doelstelling om de toezichtslast voor ondernemingen te beperken. Bij de toelating (de autorisatie): het werk van de NCCA voor de toelating invoegen in het werk van de RvA met betrekking tot de accreditatie. De NCCA vervult dan de rol van expert in het accreditatietraject om additionele schema-eisen zoals competenties te toetsen. Dat betekent dat wanneer een partij is geaccrediteerd, de toelating een formaliteit kan zijn."

Fabrikanten en dienstverleners hebben een beperkte ruimte om certificeringseisen te interpreteren en te implementeren.

Hoe beoordeelt het AT wat precies CSA-gecertificeerde producten-, diensten- en processen zouden moeten zijn? Welke kaders hanteert de NCCA?

"De NCCA heeft niet zelfstandig de mogelijkheid om eenzijdig Europese regels aan te passen. De certificeringschema's schrijven de eisen voor, waarop de NCCA toetst. Andere EU-regelgeving (zoals de NIS en CRA) zal verplichtingen tot certificering of tot gebruik van gecertificeerde producten en diensten gaan bevatten. Het AT/NCCA is deelnemer in de Europese Cybersecurity Certification Group (ECCG), die zorgt voor de ontwikkeling en beheer van de schema's. Het ECCG is in de CSA genoemd als officieel adviesorgaan van de Europese Commissie, het dagelijks bestuur van de Europese Unie op het gebied van cybersecurity. Het Europees Agentschap voor netwerk- en informatiebeveiliging ENISA krijgt opdracht van de EC tot ontwikkeling van een schema en betrekt dan externe experts en de ECCG-leden, de lidstaten, bij de ontwikkeling in een Ad Hoc Working Group (AHWG)."

Bezitten de ondernemingen die een certificaat aanvragen eigen beoordelingsruimte?

"Nee. In beginsel zijn certificeringseisen zeer concreet, de certificerende instelling interpreteert voor zover er ruimte is. Op de achtergrond kijkt de NCCA mee. Als gebreken blijven, zal het AT in haar rol als NCCA actie ondernemen met als doel het herstel van de veiligheid van een product of dienst. Ultimo kan dat leiden tot boetes, maar voordat daartoe wordt overgegaan is er al veel met elkaar gesproken. Er wordt eerst onderzoek gedaan en daarna volgt overleg en het geven van aanwijzingen. De CSA verplicht de betrokken organisaties de instantie volledige en juiste informatie aan te leveren, zo niet, dan kan het AT het certificaat in laten trekken en de Europese registratie schorsen."

"Fabrikanten en dienstverleners hebben een beperkte ruimte om certificeringseisen te interpreteren en te implementeren. Die ruimte zit voornamelijk in de keuze voor gebruikte technologie of wijze waarop een proces is ingericht. Dat is de aard van certificering. Indien een certificaathouder niet voldoet aan de eisen dan zal deze in veel gevallen de gelegenheid krijgen om dit binnen redelijke termijn te herstellen, maar het is ook mogelijk dat het certificeringsschema voorschrijft dat bij bepaald type non-conformiteit het certificaat direct moet worden ingetrokken en dat na herstel hercertificering nodig is. Ik verwacht dat in de meeste gevallen de mogelijkheid van verlies van het certificaat voorkomt dat er boetes moeten worden opgelegd."

Welke zorgen en aandachtspunten ziet het AT nu op de markten?

"Neem de certificatie-eisen op in de eigen inkoopvoorwaarden. Certificering kost tijd en is niet meer vrijblijvend. De Network & Information Security-2 directive zal verwijzen naar CSA-schema's. Dat betekent de mogelijkheid van het ontstaan van verplichtingen voor de vitale partijen."
De boodschap van Van den Bosch, als projectleider NCCA, aan de afnemers: "Kijk eens waar je zelf aan moet voldoen. Analyseer de eigen inkoopvoorwaarden daarop. Wordt actief. De hyperscalers vind je nu al actief in overleg, ook al moeten zij het nodige nog uitvinden."

Kunnen het AT, de NCCA en de informatiebeveiligers elkaar helpen? Zo ja, hoe ziet u dat?

"Allereerst kan uw lezer aandacht vragen voor deze ontwikkeling bij zijn of haar relaties en daar waar nodig de relatie en/of organisatie van advies dienen. Komt men in de markt fouten of gebreken tegen, meldt deze onregelmatigheden dan aan ons."

Drs. Johan van den Bosch MCM CISA werkt bij het Agentschap Telecom en is projectleider CSA en NCCA. Hij is bereikbaar via ncca@agentschaptelecom.nl.

Referenties

(1) ec.europa.eu/growth/single-market/goods/building-blocks/accreditation-conformity-assessment-bodies_en
(2) ITSEF: IT Security Evaluation Facility
(3) Zie ook: www.enisa.europa.eu/publications/eu-cybersecurity-market-analysis-iot-in-distribution-grid

De Nederlandse NCCA

Agentschap Telecom bereidt zich al vanaf 2019 voor op de certificerende NCCA-taken en de NCCA-toezichthoudende taken. Nederland heeft gekozen om certificerende taken volgens de CSA-optie van 'prior approval' uit te voeren, de 'voorafgaande goedkeuring'.

Agentschap Telecom als Nationale Cybersecuritycertificeringsautoriteit (NCCA)

De Nederlandse Nationale Cybersecuritycertificeringsautoriteit (NCCA) heeft een rol bij het certificeren van IT-producten, -diensten en -processen en het toezicht daarop. De Nederlandse NCCA wordt ingesteld op grond van de CSA-uitvoeringswet. De CSA-uitvoeringswet ligt bij het parlement ter behandeling. In de Memorie van Toelichting spreekt de regering het voornemen uit om de NCCA-taken bij Agentschap Telecom te beleggen.

NCCA-certificering:

- Beoordeelt of een conformiteitsbeoordelende instantie (CBI) Europese CSA-certificeringen kan en mag uitvoeren (toelating);
- Beoordeelt op het CSA-zekerheidsniveau 'hoog' of een CBI aan het einde van het certificeringstraject een Europees certificaat mag uitreiken (voorafgaande goedkeuring);
- Beoordeelt of een geaccrediteerde CBI toestemming mag geven aan de fabrikant om het 'Common Criteria Recognition Arrangement' (CCRA) logo te gebruiken bij communicatie over een gecertificeerd product.

NCCA-toezicht:

- Houdt toezicht op de naleving van de certificeringsvereisten door fabrikanten en aanbieders die een IT-product, -dienst of -proces hebben laten certificeren;
- Houdt toezicht op de naleving van de certificeringsvereisten door de toegelaten CBI's.

De Europese certificeringregelingen zijn nog in ontwikkeling. De opbouw van de NCCA-taken bij Agentschap Telecom strekt zich daarom over meerdere jaren uit. Met elk nieuwe Europees certificeringsschema (1(groeit de omvang van de NCCA-taken van Agentschap Telecom. Het eerste certificeringsschema is het EUCC-schema voor certificering van IT-producten. ENISA heeft het kandidaatschema opgeleverd aan de Europese commissie die de tekst verwerkt in een Europese regeling onder de CSA. De verwachting is dat de regeling begin 2022 wordt gepubliceerd.

Context CSA

In juni 2019 is de Europese 'Cybersecurity Act' (CSA) van kracht geworden. De CSA is een verordening waarmee de Europese Unie grensoverschrijdende cyberaanvallen beter het hoofd wil bieden. Onder de CSA-certificeringsschema's kunnen IT-producten, -diensten en -processen gecertificeerd worden op het gebied van cybersecurity. De rol van Nederlandse Nationale Cybersecuritycertificeringsautoriteit (NCCA) is ondergebracht bij Agentschap Telecom. Agentschap Telecom geeft hiermee invulling aan de certificerings- en toezichtstaken uit CSA.

Europese CSA-certificaten

Afnemers van CSA-gecertificeerde producten, -diensten en processen krijgen de zekerheid dat deze voldoen aan de cybersecurity-eisen uit de certificeringsregeling. Het is voor de aanbieders, fabrikanten en dienstverleners daarom interessant om gecertificeerde producten, diensten of processen op de markt te brengen. Europese CSA-certificaten voor IT-producten, -diensten en -processen worden erkend in elke EU-lidstaat. Hierdoor maakt een fabrikant geen kosten voor certificering in elke afzonderlijke lidstaat. Momenteel is CSA-certificering nog vrijwillig, maar op termijn verandert dat waarschijnlijk. In sommige gevallen zullen afnemers door andere nationale of Europese regelgeving verplicht worden om CSA-gecertificeerde producten-, diensten- en processen af te nemen.

Referentie

(1) www.agentschaptelecom.nl/onderwerpen/cybersecurity-certificering