N Cybersec strat A1
MH/JC/AS
940-2024

Brussel, 24 september 2024

ADVIES

betreffende

DE VOORBEREIDING VAN DE NATIONALE CYBERSECURITY STRATEGIE 2026-2030

Het Centrum Cybersecurity België (CCB) heeft het advies van de Hoge Raad voor de Zelfstandigen en de KMO gevraagd ter voorbereiding van de nieuwe nationale cybersecurity strategie voor de periode 2026-2030. Na raadpleging van de permanente werkgroep Digitalisering, Cyberveiligheid en GDPR heeft het bureau van de Hoge Raad op 24 september 2024 bij hoogdringendheid onderstaand advies uitgebracht.

CONTEXT

Het Centrum voor Cybersecurity België (CCB) heeft de input van de Hoge Raad gevraagd voor een nieuwe nationale cybersecurity strategie voor de periode 2026-2030. De lopende nationale strategie, de Nationale Cybersecurity Strategie 2.0[1], werd in 2021 door de Nationale Veiligheidsraad goedgekeurd en loopt van 2021 tot 2025. Aangezien die termijn dus volgende jaar afloopt en de nieuwe Europese NIS-2 richtlijn bovendien nieuwe verplichtingen oplegt waaraan nationale cybersecurity strategieën moeten voldoen, is een nieuwe herziene Belgische cybersecuritystrategie nodig. Het CCB is als nationale autoriteit verantwoordelijk voor het opstellen van die strategie. In zijn adviesvraag wijst het CCB erop dat de huidige aanpak erin bestaat om het cyberbeleidsdomein op te delen in vier deelgebieden: cybersecurity (Preventie-Bescherming-Reactie), cybercrime bestrijding, cyberdefensie en cyberdiplomatie. Het CCB werkt enkel aan een strategie specifiek voor het cybersecurity domein. Het CCB merkt in zijn adviesvraag tevens op dat ze in de volgende strategie een focus op dienstverlening wenst te leggen. Het CCB vraagt dan ook de mening, suggesties en algemene input van de Hoge Raad rond welke doelstellingen of dienstverleningen zouden kunnen opgenomen worden in een volgende cybersecuritystrategie.

Cyberveiligheid is voor de Hoge Raad geen nieuw onderwerp. De Hoge Raad en de erkende beroeps- en interprofessionele organisaties die bij hem vertegenwoordigd zijn, werken zelf ook mee aan het verbeteren van de cyberveiligheid van de kmo's. Intern brengt de Hoge Raad zijn leden samen rond dit onderwerp in een permanente werkgroep Digitalisering, Cyberveiligheid en GDPR. Sinds 2018 is de Hoge Raad lid van de Belgische Cyber Security Coalition (CSC) waar overheidsorganisaties, ondernemingen en de academische wereld de krachten bundelen. De Hoge Raad werkt ook nauw samen met het CCB en met de FOD Economie om de cyberveiligheid van de kmo's te verbeteren. De Hoge Raad maakt deel uit van de National Cybersecurity Council Belgium (NCCB) van het CCB. Bij de FOD Economie is de Hoge Raad nauw betrokken bij de voorbereiding en uitvoering van het Cyber4SME programma. De Hoge Raad wil hier in het bijzonder wijzen op zijn van advies van 2021 over het overheidsbeleid voor de cyberveiligheid van de kmo's[2]. In dat advies heeft hij de principes, richtlijnen en aandachtspunten geformuleerd waarmee volgens hem bij dat beleid rekening dient gehouden te worden en hij heeft daaraan ook een aantal concrete voorstellen tot actie gekoppeld. Bijna alle standpunten uit dat advies zijn ook vandaag nog relevant. Een aantal ervan worden kort in dit nieuwe advies hernomen.

[1] Online raadpleegbaar via deze link
[2] HRZKMO advies nr. 845 van 16 februari 2021 (bekrachtigd door de algemene vergadering van 6 mei 2021) over het overheidsbeleid voor de cyberveiligheid van de kmo's (online raadpleegbaar via deze link)

STANDPUNTEN

1. Goed om stakeholders te betrekken

De Hoge Raad vindt het een goede zaak dat het CCB bij de voorbereiding van de nationale cybersecurity strategie in een vroeg stadium de stakeholders betrekt en om input vraagt. Dat zal bijdragen tot een betere strategie en ook het draagvlak voor die strategie en de uitvoering ervan vergroten.

Ook in de nieuwe strategie wordt die nauwe samenwerking met de verschillende stakeholders, en met name met zij die de kmo's vertegenwoordigen, best uitdrukkelijk opgenomen. Een cybersecurity strategie zal enkel maar succesvol zijn als alle betrokken actoren samenwerken. Dat ligt ook in het verlengde van de huidige visie en manier van werken van het CCB.

De Hoge Raad vraagt dat ook het ontwerp van de strategie ter advies zou voorgelegd worden.

2. Aandacht voor kmo's en hun eigenheid

Er is de voorbije jaren door alle betrokken actoren reeds heel wat werk ondernomen om de cyberveiligheid van kmo's te vergroten. Dat werk heeft impact gehad. Meer kmo's zijn zich bewust van cyberrisico's en hebben alvast enkele maatregelen genomen. Over het algemeen blijft het bewustzijn en de cyberweerbaarheid van kmo's echter zeer laag. Bovendien zijn de cyberbedreigingen en -risico's toegenomen.[3] De uitdaging om de cyberveiligheid van kmo's te verhogen, is er dus niet minder op geworden. Bovendien moet opgemerkt worden er in België ca. 1.144.000 ondernemingen zijn, waarvan ca. 1.136.000 of 99,3% kmo's zijn (< 50 werknemers).[4] Deze kmo's vormen de ruggengraat van onze economie. Volgens de Hoge Raad dienen ze binnen de nieuwe nationale cybersecurity strategie dan ook bijzondere aandacht te krijgen.

Tevens moet men rekening houden met de eigenheid van de kmo's. 99,3% van de Belgische ondernemingen zijn dus kmo's maar 96,7% van de Belgische ondernemingen zijn micro-ondernemingen (< 10 werknemers) en 83% hebben geen personeel. Kmo's en zeker de micro-ondernemingen en eenmanszaken werken op een totaal andere manier dan grote ondernemingen. Zo hebben ze vaak geen eigen ICT-dienst en kennen ze een aantal schaalnadelen. De Hoge Raad pleit dan ook voor een beleid en voor informatie en steunmaatregelen op maat van de kmo's.

Bijzondere aandacht voor de kmo's, komt bovendien niet alleen de kmo's maar de volledige supply chain ten goede. Kmo's, zeker deze zonder eigen ICT-dienst, lopen een groter risico om het slachtoffer van een cyberaanval te worden en kunnen zo ook ongewild een gevaar vormen voor de andere (grotere) ondernemingen in de supply chain waar zij deel van uitmaken. Als de overheid deze kmo's extra ondersteunt, zal dat dus alle ondernemingen ten goede komen.

[3] Zie onder meer de meest recente EWI CS-barometer en het UNIZO rapport Digitale fitheid 2024
[4] Bron: Statbel - FOD Economie, K.M.O., Middenstand en Energie. Situatie op 31/12/2022

3. Preventieve, beschermende maatregelen

De Hoge Raad meent dat wat kmo's betreft, het best gekozen wordt voor beschermende maatregelen. In zijn adviesvraag maakt het CCB onderscheid tussen preventie, bescherming en reactie. Het is voor de Hoge Raad niet helemaal duidelijk wat in dat geval het onderscheid tussen preventie en bescherming is. Zelf vertrekt de Hoge Raad doorgaans van de zes domeinen van het NIST Cybersecurity Framework 2.0: identify, protect, detect, respond, recover en govern. Hoewel alle domeinen aandacht vragen, wordt er voor kmo's in de eerste plaats best ingezet op acties die de bescherming ten goede komen. Dergelijke acties zijn per definitie ook preventief. De impact van een cyberincident op een kmo is doorgaans zo ernstig dat preventieve acties de voorkeur genieten.

Die acties moeten zich richten op zowel de menselijke, technologische als procesmatige elementen van cyberveiligheid. Veel cyberincidenten zijn het gevolg van menselijke vergissingen of keuzes. Kmo's kunnen echter op een relatief gemakkelijke wijze, bijvoorbeeld door trainingen op het vlak van basis cyberhygiëne, die menselijke factor terugdringen en hun cyberveiligheid gevoelig verhogen. Technologie en processen spelen echter ook een belangrijke rol. Een kmo zal dus aandacht moeten hebben voor de drie soorten acties.

De Hoge Raad pleit er ook voor verder in te zetten op strategieën en technologieën die de ondernemer beschermen zonder dat hij daar zelf iets voor moet doen of zich daar zorgen moet over maken. Hij steunt dan ook CCB projecten zoals het Belgian Anti-Phishing Shield, stop smishing en spear warning. Er moet nog altijd ingezet worden op het sensibiliseren en trainen van kmo's en hun personeel. Het is echter nog beter indien een dreiging kan weggenomen worden vooraleer die bij de kmo's geraakt of wanneer kmo's zeer gericht kunnen geïnformeerd worden over specifieke dreigingen.

De Hoge Raad onderstreept eveneens dat het belangrijk is de cyberveiligheid te garanderen van de software die door kmo's gebruikt wordt. Kmo's moeten kunnen vertrouwen op de software die ze gebruiken, zeker als ze die ter beschikking stellen van hun eigen klanten.

Wat de te kiezen maatregelen betreft, is de Hoge Raad dan zeker ook voorstander van de Active Cyber Protection (ACP) strategie van het CCB[5] die staat voor een proactieve, op maat gemaakte, geautomatiseerde en participatieve benadering.

4. Hoe kmo's bereiken?

Er zijn heel veel kmo's en hoewel ze meestal slechts met één of enkele personen zijn, krijgen ze erg veel informatie over zeer uiteenlopende onderwerpen te verwerken. Kmo's zijn daarom erg moeilijk te bereiken of tot actie aan te zetten. Een belangrijke vraag is dan ook via welke kanalen het beste kan gecommuniceerd worden.

De Hoge Raad is er van overtuigd dat in de eerste plaats de kmo-organisaties een zeer goed kanaal vormen. Ze kennen hun leden, hebben hun vertrouwen en beschikken over de nodige communicatiekanalen. In het geval van beroepsorganisaties, worden de leden daarenboven vaak met erg gelijkaardige uitdagingen op het vlak van ICT en cyberveiligheid geconfronteerd. De

[5] ccb.belgium.be/sites/default/files/documents/ACP_Policy_Document_EN.pdf

beroepsorganisaties zijn dan ook de meest aangewezen partners om de kmo's te informeren en om hen te helpen hun cyberweerbaarheid te verhogen. De overheid moet de kmo-organisaties daar actief bij ondersteunen.

In de tweede plaats denkt de Hoge Raad ook aan de ICT-dienstverleners. Veel kmo's doen beroep op ICT-dienstverleners. Deze zijn dan ook de aangewezen partner om de kmo's te helpen hun cyberveiligheid te verbeteren. Aangezien deze ICT-dienstverleners echter ook niet allemaal daarvoor de nodige kennis en competenties hebben, vraagt de Hoge Raad dat er ook projecten zouden ontwikkeld worden om de ICT-dienstverleners te helpen die rol op te nemen.

Daarnaast heeft nagenoeg elke kmo ook een telecomoperator, bank, verzekeraar en vaak ook een accountant. Ook via die kanalen kan men de kmo's bereiken.

Tot slot is de Hoge Raad van mening dat kleine ondernemingen ook best lokaal geïnformeerd en ondersteund worden. Via de lokale ondernemersverenigingen, via de diensten Integrale veiligheid van de steden en gemeenten en via de politiezones van de lokale politie kunnen ondernemers bereikt worden die via de andere kanalen moeilijk bereikt kunnen worden. Zoals er bijvoorbeeld reeds in veel steden en gemeenten advies inzake inbraakpreventie wordt gegeven, zou er ook advies inzake cyberveiligheid voor kleine ondernemers moeten worden aangeboden. De Hoge Raad zal hierover nog een afzonderlijk advies uitbrengen en ondersteunt ook een proefproject op dat vlak.

5. Cyberveiligheid als deel van digitalisering

Verder digitaliseren is ook een uitdaging voor veel kmo's. In plaats van digitalisering en cyberveiligheid als twee verschillende uitdagingen te benaderen, kan best ingezet worden op cyberveilige digitalisering: Hoe kan een kmo zich zo best mogelijk digitaal organiseren? En hoe doet die dat cyberveilig? Dat is een logische 'by design' benadering van cyberveiligheid. Bovendien motiveert die insteek kmo's sterker om actie te ondernemen omdat de voordelen die ze van verdere digitalisering hebben zichtbaarder zijn. Aangezien de kmo's binnen eenzelfde sector met soortgelijke digitale uitdagingen geconfronteerd worden, ondersteunt de overheid hen daarbij dan ook best via de beroepsorganisaties.

6. Digitale vaardigheden personeel en klanten

De kmo-ondernemer moet zijn digitale vaardigheden versterken maar de cyberveiligheid van de kmo is ook afhankelijk van verschillende andere groepen zoals het personeel, de klanten en de ICT-dienstverleners. In alle vormen van onderwijs en opleiding moet dan ook meer aandacht uitgaan naar digitale vaardigheden waaronder cyberveiligheid. Als de klant van de kmo slachtoffer wordt van cyberfraude, straalt dat ook af op of kan dat ook gevolgen hebben voor de betrokken kmo. De burger / klant is vaak de zwakste schakel en de Hoge Raad is dan zeker ook voorstander dat de overheid nog meer inzet op het informeren en ondersteunen van de burger.

7. Een cybersecurity helpdesk voor kmo's

De Hoge Raad vraagt de CERT-functie van het CCB[6] uit te breiden naar alle ondernemingen. Alle kmo's zouden bij het CCB moeten terecht kunnen voor eerste lijnsadvies in het geval van een cyberincident.

Kmo-organisaties zijn in veel gevallen ook een eerste aanspreekpunt voor ondernemers wanneer zij vragen of problemen hebben. Een aantal kmo-organisatie hebben daarvoor zelf een call center opgericht. Via die weg komen bij hen dus ook heel wat vragen en meldingen met betrekking tot cyberincidenten terecht. Het is belangrijk dat zij deze op een systematische wijze kunnen doorgeven aan het CCB en er daarvoor een samenwerking wordt aangegaan.

8. Bij certificering rekening houden met kmo's

De Hoge Raad erkent het nut dat certificaten en labels kunnen hebben op het vlak van cyberveiligheid. Voor kmo's is het, door hun kleinere schaal, echter moeilijker dan voor grote ondernemingen om dergelijke certificaten of labels te behalen. De Hoge Raad verzet zich dan zeker ook tegen verplichtingen voor kmo's op het vlak van certificaten of labels. Kmo's moeten in de eerste plaats gestimuleerd en ondersteund worden om hun cyberveiligheid te verbeteren. Labels of certificaten kunnen daarbij, als vrijwillige instrument, nuttig zijn voor kmo's.

In de gevallen waar certificaten of labels wel noodzakelijk en verplicht zijn (bijvoorbeeld indien men onder het toepassingsgebied van de NIS2-richtlijn valt), pleit de Hoge Raad voor instrumenten die aangepast zijn aan en haalbaar zijn voor de kmo's.

Certificaten en labels kunnen ook een oplossing bieden voor het zogenaamde trickle down effect, dus wanneer grote ondernemingen omwille van hun eigen verplichtingen de kmo's met wie ze samenwerken (uiteenlopende) rapporteringsverplichtingen opleggen of (moeilijk te behalen) certificaten vragen. In die gevallen kan een eenvoudige en uniforme KMO-standaard een oplossing bieden en de situatie voor zowel de kmo's als de grote ondernemingen vereenvoudigen.

Omwille van die verschillende redenen, steunt en promoot de Hoge Raad dan ook het CyberFundamentals Framework initiatief[7] van het CCB. Dit kader heeft als voordeel dat het goed onderbouwde labels op verschillende niveaus (Small, Basis, Belangrijk, Essentieel) voorziet, zodat ook kmo's ze kunnen gebruiken.

Zoals eerder aangehaald, is het voor kmo's bovendien erg belangrijk dat zij kunnen vertrouwen op de software die zij gebruiken en op de ICT-diensten die zij afnemen. Ook daarvoor kunnen certificaten en labels of andere kwaliteitsgarantiesystemen een oplossing bieden.

9. De impact van maatregelen beoordelen

De Hoge Raad is er voorstander van dat beleidsmaatregelen ex ante en ex post geëvalueerd worden. In het geval van maatregelen om de cyberveiligheid van kmo's te verhogen, is het dan wel belangrijk om naar de reële impact te kijken. De ervaring toont aan dat het erg moeilijk is om kmo's te overtuigen deel te nemen aan initiatieven om hun cyberveiligheid te verhogen. In

[6] Cyber Emergency Response Team (https://ccb.belgium.be/nl/cert)
[7] https://atwork.safeonweb.be/nl/tools-resources/cyberfundamentals-framework

verschillende projecten worden dan ook slechts beperkte aantallen kmo's bereikt. Bij het meten van de impact van een project moet echter niet louter gekeken worden naar het aantal bereikte kmo's. Cyberincidenten kunnen een zeer grote impact voor een kmo hebben en zeer hoge kosten met zich meebrengen. De impact van beleidsmaatregelen moeten dan ook gemeten worden in termen van vermeden schade.

10. Coördinatie tussen overheidsactoren

Bij cyberveiligheid zijn verschillende beleidsniveaus en overheidsactoren betrokken. Dat is positief aangezien er op deze manier veel middelen kunnen ingezet worden. Anderzijds is er duidelijk nood aan meer afstemming en een meer uniforme strategische en operationele aanpak.

Kmo's vrageneenvoudige en eenduidige informatie en steun. Voor hen wordt het net moeilijker als ze vanuit verschillende hoeken soortgelijke informatie en ondersteuning krijgen aangeboden. Momenteel vinden kmo's informatie en steunmaatregelen van de overheid bij zowel het CCB, de FOD Economie als de regionale organisaties VLAIO, AdN en hub.brussels. Die informatie en steun zou hen beter gegroepeerd op één website aangeboden worden. Ten minste zou men ergens een overzicht van alle maatregelen moeten aanbieden en zouden de verschillende initiatieven en websites naar dat overzicht of naar elkaar moeten doorverwijzen. Een goede afstemming in alle fases van de beleidscyclus en tussen alle betrokken actoren is noodzakelijk.

11. Gezamenlijke statistieken

Er is nog steeds een groot tekort aan gegevens inzake cyberrisico's en -incidenten. Die gegevens zijn nochtans belangrijk voor ondernemingen en ondernemingssectoren om weloverwogen beslissingen te nemen. Ook de overheid kan alleen maar een efficiënt en effectief beleid voeren indien ze over voldoende beleidsondersteunende data beschikt. De bestaande informatie is verspreid en gebaseerd op verschillende methodologieën en typologieën. De Hoge Raad vraagt dat bij het CCB of de Cyber Security Coalition een werkgroep wordt opgericht die als doel heeft de beschikbaarheid van gegevens inzake cyberrisico's en -incidenten te verbeteren. Deze werkgroep kan alle betrokken publieke en private partners samenbrengen, de beschikbare data en hiaten in kaart brengen, gezamenlijk methodologieën en typologieën ontwikkelen, enz.

12. Multidisciplinair onderzoek

Het is belangrijk dat België investeert in onderzoek naar cyberveiligheid. Zeker de combinatie van cyberveiligheid en AI lijkt een interessant speerpunt voor onderzoek. Volgens de Hoge Raad is het bovendien interessant om niet alleen in technologisch onderzoek te investeren maar ook in onderzoek dat aandacht heeft voor minder technische aspecten zoals awareness, kmo-eigenheid, gedragsinzichten, de kosten van cybercriminaliteit voor ondernemingen, enz. Zoals

ondernemingen cyberveiligheid niet enkel vanuit ICT-oogpunt maar multidisciplinair moet aanpakken, moet ook bij het onderzoek door universiteiten en hogescholen voor een multidisciplinaire aanpak gekozen worden.

13. Cyberverzekeringen

De Hoge Raad ziet cyberverzekeringen niet als alleenstaande oplossingen maar wel als een sluitstuk van een reeks cyberveiligheidsmaatregelen die een organisatie of burger neemt. De markt van cyberverzekeringen evolueert snel. Het is aangewezen dat de overheid samen met de betrokken actoren deze markt monitort. Tevens zou onderzocht moeten worden of er in bepaalde gevallen geen andere solidariteitsmechanismen kunnen opgezet worden, zoals bijvoorbeeld een noodfonds. In dit kader vraagt de Hoge Raad ook dat er wordt op toegezien dat alle spelers hun verantwoordelijkheid opnemen. Zo zijn er veel signalen dat banken in het geval van bankfraude te gemakkelijk de schuld bij de kmo-klant leggen en de schade niet willen vergoeden.

BESLUIT

De Hoge Raad vraagt dat de kmo's, die de ruggengraat van onze economie vormen, binnen de nieuwe nationale cybersecurity strategie bijzondere aandacht krijgen. De cyberveiligheid van kmo's is over het algemeen zeer laag, terwijl de cyberbedreigingen en -risico's alleen maar zijn toegenomen. Daarbij moet tevens rekening gehouden worden met de eigenheid van de kmo's. Ze hebben nood aan informatie en steunmaatregelen op maat van kmo's. Vanuit die optiek formuleert de Hoge Raad in dit advies een reeks standpunten inzake de doelstellingen en diensten van het CCB. De Hoge Raad vraagt dat bij het opstellen van de nationale strategie daar rekening mee gehouden wordt.