N cyber A2 **Brussel, 6 mei 2021**
MH/JC/AS
845-2021

ADVIES

over

HET OVERHEIDSBELEID VOOR DE CYBERVEILIGHEID VAN DE KMO'S

(goedgekeurd door het bureau op 16 februari 2021,
bekrachtigd door de algemene vergadering van de Hoge Raad op 6 mei 2021)

Cyberveiligheid vormt een belangrijke uitdaging voor de zelfstandigen en de kmo's. Vandaar heeft de Hoge Raad voor de Zelfstandigen en de KMO beslist op eigen initiatief een advies uit te brengen over het overheidsbeleid voor de cyberveiligheid van de kmo's. Na besprekingen in de commissie ad hoc Cyberveiligheid, heeft het bureau van de Hoge Raad op 16 februari 2021 onderstaand advies uitgebracht, dat werd bekrachtigd door de algemene vergadering van de Hoge Raad op 6 mei 2021.

INLEIDING

1. Een belangrijke beleidsprioriteit

Cybercriminaliteit vormt voor zelfstandigen en kmo's een reële bedreiging. Tegelijkertijd weten we dat ze veel minder beschermd zijn. Cybercriminaliteit kan nochtans erg belangrijke kosten voor de onderneming tot gevolg hebben en zelfs haar continuïteit in het gedrang brengen. Zowel cybercriminaliteit als de maatregelen om zich daartegen te beschermen brengen belangrijke kosten met zich mee voor de Belgische ondernemingen en de Belgische economie. Ook in het kader van de Algemene Verordening Gegevensbescherming en de verplichtingen die deze regelgeving aan de kmo's oplegt, speelt cyberveiligheid een belangrijke rol. Cyberveiligheid en meer algemeen digitaal vertrouwen zijn bovendien belangrijke voorwaarden voor de verdere digitalisering van onze economie en voor de groei van de digitale economie. De cyberveiligheid van de zelfstandigen en de kmo's is dan ook terecht een belangrijke beleidsprioriteit geworden waar absoluut verder moet op ingezet worden.

2. Een complex probleem

Het verhogen van de cyberveiligheid van de ondernemingen is een complex probleem dat veel facetten kent en waar heel wat actoren bij betrokken zijn.

Er is enerzijds de bestrijding van cybercriminaliteit en anderzijds de bescherming tegen cybercriminaliteit of het verhogen van de cyberweerbaarheid van de ondernemingen. Er stellen zich uiteenlopende economische, juridische, technologische, maatschappelijke en ethische uitdagingen. De cyberbescherming binnen de onderneming bestaat naast een technologische component ook uit een belangrijke menselijke component, de zogenaamde 'human error'. Cybercriminaliteit is een internationaal, grensoverschrijdend probleem.

Bij de bestrijding van cybercriminaliteit en bij cyberbescherming zijn tal van private en publieke actoren betrokken. De kmo's zelf worden niet alleen als (potentiële) slachtoffers gezien maar ook als medeverantwoordelijk voor hun eigen bescherming en de bescherming van hun klanten, personeelsleden en partners. Ook leveranciers en dienstverleners, klanten en personeelsleden spelen een rol. Aan overheidszijde zijn verschillende beleidsdomeinen en -niveaus betrokken. Dat er veel verschillende actoren betrokken zijn, hoeft echter niet noodzakelijk een nadeel te zijn maar kan evengoed als een opportuniteit benut worden om veel inzet en middelen te mobiliseren. Voorwaarde is echter wel een minimale afstemming en samenwerking.

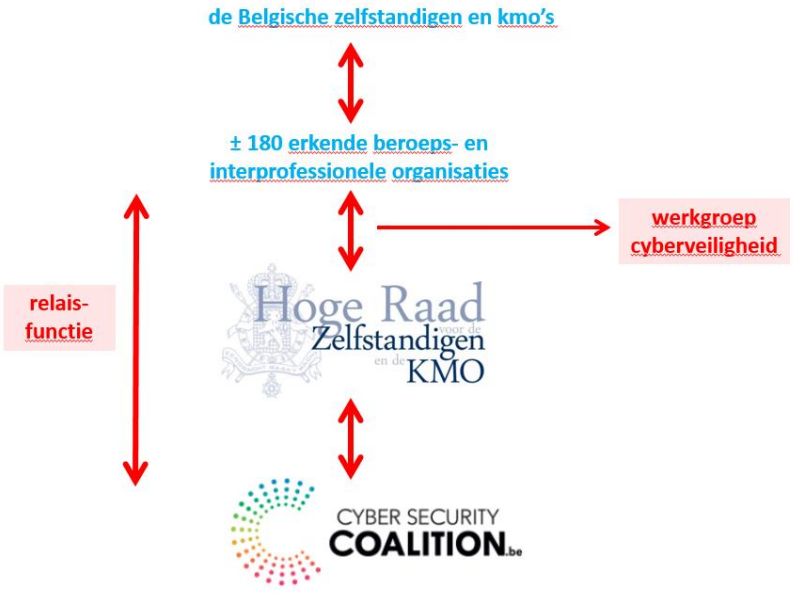
3. Actieve rol van de HRZKMO en zijn leden

De Hoge Raad voor de Zelfstandigen en de KMO en de erkende beroeps- en interprofessionele organisaties die bij hem vertegenwoordigd zijn, werken zelf ook mee aan het verbeteren van de cyberveiligheid van de zelfstandigen en de kmo's.

Sinds januari 2018 is de Hoge Raad lid van de Belgische Cyber Security Coalition (CSC) in het kader waarvan overheidsorganisaties, ondernemingen en de academische wereld de krachten bundelen. De vraag stelde zich namelijk hoe de kmo's beter binnen de CSC konden vertegenwoordigd worden. Uit overleg met alle betrokken actoren kwam naar voren dat de Hoge Raad daarin best een rol zou opnemen. Vandaar dat de Hoge Raad lid is geworden van de CSC. Het secretariaat van de Hoge Raad vertegenwoordigt de bij hem vertegenwoordigde beroeps- en interprofessionele organisaties bij de CSC en vervult een verbindingsrol tussen de CSC en deze organisaties. Deze organisaties kunnen daarnaast natuurlijk ook rechtstreeks lid van de CSC worden en aldus de directe voordelen van een lidmaatschap genieten. Concreet vertaalt het lidmaatschap van de Hoge Raad bij de CSC zich in een actieve deelname aan de activiteiten en aan verschillende focusgroepen van de CSC.

Intern bij de Hoge Raad werd er (onder de vorm van een commissie ad hoc) een permante werkgroep Cyberveiligheid opgericht met daarin vertegenwoordigers van verschillende van de bij hem vertegenwoordigde beroeps- en interprofessionele organisaties. Deze werkgroep heeft als hoofddoelstelling de cyberveiligheid van de zelfstandigen en de kmo's te verbeteren en heeft zich daartoe volgende subdoelstellingen gesteld: standpunten voorbereiden, de relaisfunctie HRZKMO-CSC ondersteunen, expertise opbouwen, samenwerking promoten en andere actoren ondersteunen in hun streven naar cyberveiligheid voor kmo's.

Onderstaand schema geeft deze samenwerkingsrelaties weer.



De Hoge Raad en zijn leden ondernemen ook zelf acties gericht op het informeren, sensibiliseren en ondersteunen van de zelfstandigen en de kmo's inzake cyberbescherming, bijvoorbeeld door het organiseren van info-events, het verspreiden van instrumenten van de CSC of door mee te werken aan de campagnes van het Centrum voor Cyberveiligheid België.

Visie op KMO-cyberveiligheid

Het is niet de bedoeling in dit advies een uitgebreid actieplan voor te stellen van maatregelen die door de overheid dienen genomen te worden om de cyberveiligheid van de zelfstandigen en de kmo's te verbeteren. In dit advies wil de Hoge Raad in de eerste plaats zijn visie delen op de cyberveiligheid van de zelfstandigen en kmo's en meer bepaald dan op het daarop gerichte overheidsbeleid. Hij formuleert hier dan ook de principes, richtlijnen en aandachtspunten waarmee volgens hem bij dat beleid dient rekening gehouden te worden en koppelt daaraan alvast een aantal concrete voorstellen tot actie.

1. Een reëel probleem

Cybercriminaliteit vormt voor de Belgische zelfstandigen en kmo's een reëel probleem. Uit alle beschikbare cijfers blijkt de ernst van het probleem alsook de het feit dat de risico's jaar na jaar toenemen. Kmo's onderschatten de risico's echter en beschouwen zichzelf doorgaans niet als een doelwit voor cybercriminelen. In tegenstelling tot fysieke criminaliteit is cybercriminaliteit veel minder zichtbaar en ondernemers die slachtoffer werden van cybercriminaliteit zijn ook veel minder snel geneigd daarover te communiceren uit vrees voor imagoschade en het verlies van het vertrouwen van hun klanten en partners.

Het is dan ook noodzakelijk kmo's blijvend te informeren en te sensibiliseren over het risico dat ze lopen. Een concrete actie waar de Hoge Raad vragende partij voor is, is een campagne opgebouwd rond getuigenissen van kmo's die slachtoffer werden van cybercriminaliteit. Het is ook belangrijk om de meldingsbereidheid bij kmo's te verhogen. Een goede dataverzameling inzake cyberincidenten en een gezamenlijke typologie voor cyberincidenten die door alle actoren gebruikt wordt, zouden ook helpen om de cyberincidenten waarmee kmo's geconfronteerd worden beter in kaart te brengen en hen zo te overtuigen van de risico's die ze lopen.

2. Overgrote meerderheid van de ondernemingen zijn kleine ondernemingen

Wanneer er over cyberveiligheid en meer algemeen over digitalisering wordt gesproken, wordt er vaak vergeten dat de overgrote meerderheid van de Belgische ondernemingen kleine ondernemingen zijn. Bovendien hebben het merendeel van deze ondernemingen geen eigen ICT-verantwoordelijke. 99% van Belgische ondernemingen tellen minder dan 50 werknemers. Hoewel de Europese KMO-definitie kmo's aanduidt als ondernemingen met minder dan 250 werknemers, wordt er in de Belgische context met kmo's doorgaans nog verwezen naar ondernemingen met minder dan 50 werknemers, zijnde dus de ondernemingen die in het kader van de Europese definitie als kleine ondernemingen worden aangeduid. Bovendien zijn, zoals onderstaande cijfers tonen, heel wat van die ondernemingen micro-ondernemingen met minder dan 10 of geen personeelsleden. Beleidsinitiatieven die zich tot ondernemingen richten, moeten (overeenkomstig het Europese Think small first-principe) de kmo's als uitgangspunt en norm nemen. In iedere geval moeten er voldoende initiatieven zijn die zich specifiek op deze grote groep van kleine ondernemingen richten.

99 %

van de Belgische ondernemingen zijn kmo's (< 50 WN)

97 %

van de Belgische ondernemingen zijn micro-ondernemingen (< 10 WN)

	Aantal ondernemingen	%
zonder WN	823.345	81,5%
1-4 WN	121.306	12%
5-9 WN	30.347	3%
10-19 WN	17.332	1,7%
20-49 WN	11.175	1%
50-249 WN	5.513	0,6%
+250 WN	1.617	0,2%
Totaal	1.010.635	

Bron: bestat.statbel.fgov.be – Cijfers op dd. 31/12/2019

Tevens wordt in sommige beleidsdomeinen het aandeel van de hoogtechnologische en digitale ondernemingen overschat. Vanzelfsprekend verdienen die ondernemingen belangrijke beleidsaandacht en ook in andere sectoren is er geen enkele onderneming die niet in meer of mindere mate digitaliseert. Het grootste aandeel van onze economie wordt echter gevormd door niet-hoogtechnologische of niet-digitale ondernemingen en beroepen, gaande van verzekeringsmakelaars tot bouwbedrijven, die even goed met de uitdagingen inzake cyberveiligheid geconfronteerd worden. Ook dat mag men niet uit het oog verliezen bij het nemen van initiatieven om de cyberveiligheid van ondernemingen te verhogen.

Tot slot dient hier nog opgemerkt te worden dat de kmo's onderling ook nog erg sterk van elkaar verschillen zowel qua grootte, soort van de activiteit, mate van digitalisering, maturiteit inzake cyberveiligheid, risicoprofiel en de manier waarop men georganiseerd is. Binnen de groep van kmo's zal er dus ook nog een verdere segmentering moeten gebeuren.

3. Specifieke situatie kmo's

Wat cyberveiligheid betreft, bevinden de zelfstandigen en kmo's zich in een bijzondere situatie wat maakt dat ze extra door de overheid dienen ondersteund te worden:

- In de eerste plaats kan men niet anders dan vaststellen dat de gemiddelde kmo slecht beschermd is, zeker vergeleken met de grotere ondernemingen en organisaties. Dat maakt van hen een gemakkelijk slachtoffer.

- Bovendien zien we dat grotere ondernemingen en organisaties zich steeds beter beveiligen waardoor de focus van cybercriminelen zich naar de minder goed beveiligde actoren, zijnde dus de kmo's, verschuift.

- Cybercriminelen zien de kleinere ondernemingen ook als een toegangspoort tot de grotere ondernemingen en organisaties. Als ze niet meer rechtsreeks bij die grotere binnen geraken, zullen ze dat proberen via de minder goed beschermde, kleinere partners die via het internet verbonden zijn met de grotere.

- Gezien hun kleine omvang beschikken kmo's vaak niet over een eigen ICT-dienst of eigen ICT expertise binnen de onderneming. Voor hun ICT moeten zij beroep doen op externe dienstverleners. Dit kan ook het implementeren van cyberveiligheidsmaatregelen bemoeilijken.

- Kmo's hebben ook schaalnadelen. Technische maatregelen zoals de installatie van een firewall, kosten nagenoeg evenveel voor een grote als een kleine organisatie. Cyberbescherming zal dus in verhouding tot de grootte van de onderneming meer kosten voor kleine ondernemingen.

- Die kleinere schaal maakt ook dat kleine ondernemingen bij een cyberincident de gevolgen ervan moelijker zullen te boven komen. De impact van een cyberincident op hen zal groter zijn aangezien ze eenvoudigweg over minder omvang en reserves beschikken om de effecten van een cyberincident op te vangen.

- En tot slot is er de eenvoudige vaststelling dat er veel meer kmo's zijn dan grote ondernemingen waaruit logischerwijze volgt dat veel meer kleine dan grote ondernemingen met cybercriminaliteit te maken krijgen.

Het is dan ook uitermate belangrijk dat de overheden in hun cyberveiligheidsbeleid voldoende en specifieke aandacht voor de kmo's hebben.

4. Awareness en training op maat van de kmo's

De Hoge Raad is er van overtuigd dat cyberveiligheid een prioriteit moet vormen voor de zelfstandigen en de kmo's maar de gemiddelde ondernemer wordt geconfronteerd met enorm veel informatie en tal van prioritaire aandachtspunten gaande van het terugdringen van arbeidsongevallen tot sociale fraudebestrijding. De Hoge Raad pleit dan ook voor een pragmatische aanpak op maat van de kmo's die focust op preventie, awareness en training en die toelaat dat de kmo's daadwerkelijk stappen zetten richting een betere cyberveiligheid.

Er dient aandacht te gaan naar de verschillende functies of werkdomeinen van cyberveiligheid (identify, protect, detect, respond, recover) maar de nadruk moet in de eerste plaats liggen op beschermende, preventieve acties.

Naast goede en betaalbare technologische en procesmatige oplossingen op maat van de kmo's, moet er bijzondere aandacht gaan naar de menselijke factor. Door volop in te zetten op awareness en training kan men een basis cyberhygiëne nastreven en met een relatief beperkte investering van tijd en middelen toch een aanzienlijke verbetering van de cyberveiligheid van de onderneming realiseren. Bij kmo's is er echter nog heel veel werk op het vlak van awareness en training. Er moet bovendien gestreefd worden naar concrete gedragsverandering bij de ondernemers en hun personeel. Inzichten uit de gedragspsychologie en technieken zoals nudging en gamification kunnen daarvoor aangewend worden.

Informatie en instrumenten moeten op maat van de kmo's opgesteld worden.

- Het taalgebruik, de hoeveelheid en de complexiteit van informatie moeten aangepast worden. Wanneer men bijvoorbeeld in een informatiebrochure spreekt over management commitment en verwijst naar verschillende management functies, staat men ver van de praktijk van de gemiddelde Belgische kmo en loopt men het risico dat veel kmo's al onmiddellijk afhaken.

- Momenteel staat de voor kmo's relevante informatie inzake cyberveiligheid ook op verschillende plaatsen verspreid. Voor kmo's zou het handig zijn als alle voor hen nuttige informatie inzake cyberveiligheid op één website gegroepeerd wordt.

- Kmo's hebben nood aan concrete en praktische informatie en tools. De meeste kmo's hebben intern zeer weinig ICT-expertise en zeker al niet op het vlak van cyberveiligheid. Ze beschikken vaak ook niet over de middelen om daarvoor intensief beroep te doen op een externe dienstverlener. Het heeft dan ook weinig nut kmo's te vragen om tools te gebruiken of acties te nemen die voor hen niet haalbaar zijn omdat ze zelf niet over de nodige expertise daartoe beschikken of omdat daarvoor beroep doen op externe ondersteuning te duur is. Voor die acties die noodzakelijk zijn en waarvoor specifieke expertise noodzakelijk is, moet de overheid in steunmaatregelen (fiscale aftrekbaarheid, adviescheques, …) voorzien. Scans of self-assessments die de kmo adviseren bepaalde acties te ondernemen, zouden de kmo zonder interne ICT-expertise ook een checklist kunnen bieden die hij kan gebruiken om een dienstverlener te zoeken en de dialoog met die dienstverlener aan te gaan.

Zoals reeds opgemerkt vormen de kmo's bovendien geen homogene groep. In de mate van het mogelijke dient er rekening gehouden te worden met de situatie van elke individuele onderneming. Dat kan bijvoorbeeld door in scans of assessment tools te vertrekken vanuit de concrete situatie van de onderneming die er gebruik van maakt. In ieder geval zou er rekening gehouden moeten worden met de soortgelijke kenmerken van ondernemingen binnen eenzelfde beroepssector door middel van een beroepsspecifieke benadering (cf. infra).

Wat de certificatie van de cyberveiligheid bij kmo's betreft, pleit de Hoge Raad voor een voorzichtige en terughoudende benadering. Voor kmo's is het door hun kleinere schaal in vergelijking met grotere ondernemingen moeilijker om een certificaat te behalen. Voor de overgrote meerderheid van de kmo's hebben dergelijke certificaten momenteel ook weinig zin. Er dient voor hen vooral ingezet te worden op meer bewustmaking en informatie en op concreet advies op maat. Certificatie moet in ieder geval vrijblijvend zijn en overheidsinitiatieven inzake certificatie worden best gericht op die marktniches waar certificaten daadwerkelijk een toegevoegde waarde bieden omdat de ondernemingen anders geconfronteerd worden met uiteenlopende rapporteringsvereisten van hun klanten of gevraagd worden reeds bestaande, zwaardere certificaten voor te leggen. Vanuit de kmo's bestaat er bovendien ook een vraag naar meer garanties inzake de cyberveiligheid van de ICT-diensten en -producten die zij gebruiken. In dat opzicht is de certificatie van ICT-diensten, -producten en -dienstverleners wel een goede piste.

5. Zet in op technologische oplossingen

Strategieën om de cyberbescherming van kmo's te verhogen zouden er finaal op moeten gericht zijn die bezorgdheid en dat werk zo veel als mogelijk bij de kmo weg te nemen. Het feit dat de menselijke factor (human error) vaak een belangrijke rol speelt bij het ontstaan van cyberveiligheidsincidenten betekent dat de ondernemer en zijn personeel altijd deel van het verhaal zullen blijven. Anderzijds betekent dit eveneens dat die menselijke factor best zo beperkt mogelijk gehouden wordt. Er moet dus ingezet worden op strategieën en technologieën die de ondernemer beter beschermen zonder dat hij daar zelf iets voor moet doen of zich daar zorgen moet over maken.

Neem bijvoorbeeld phishing. We moeten blijven werken aan het sensibiliseren en informeren van de ondernemers maar beter is nog er voor te zorgen dat de phising mails niet tot bij de ondernemer geraken door middel van betere spam filters, het snel blokkeren van malafide websites, internationale samenwerking om de bendes die achter phishing aanvallen schuil gaan aan te pakken, enz. Ook multi-factor authentificatie en cloud oplossingen kunnen de ondernemer ontzorgen. Daarnaast bestaan er heel wat technologische oplossingen die door grote ondernemingen worden gebruikt maar doorgaans niet toegankelijk zijn voor kmo's. Denk bijvoorbeeld aan phishing tests, automated penetration testing, digital risk protection, managed detection and response, …

De Hoge Raad vraag dat de overheid maatregelen neemt om het aanbod van technologische oplossingen te versterken, om deze geschikt en toegankelijk te maken voor kmo's en om kmo's te stimuleren ze te gebruiken. De recent ontwikkelde app BeGuard van het Centrum voor Cyberveiligheid België is een voorbeeld van een op kmo's gerichte technologische oplossing die erg nuttig voor hen kan zijn. Tevens zou er moeten naar gestreefd worden dat kmo's alleen maar gebruik maken van software die aan minimale veiligheidseisen voldoet, vandaar het belang van de certificatie van software.

6. Risk assessment voor aangepaste bescherming

Kmo's hebben nood aan een cyberbescherming die aangepast is aan hun kenmerken en cyberrisico's. Kmo's moeten overtuigd worden die acties te nemen die voor hen haalbaar zijn en die daadwerkelijk hun cyberveiligheid verhogen. Er moet in ieder geval vermeden worden dat ze tijd en geld investeren in oplossingen die hen geen, te veel of verkeerde bescherming bieden. Daarom is het belangrijk te weten met welke risico's zij geconfronteerd worden.

Het uitvoeren van eenvoudige risk assessments op het niveau van de individuele kmo kan zeker gepromoot worden maar gezien de grote gelijkenissen tussen kmo's binnen eenzelfde beroepssector, is het zeker ook aangewezen dat er op niveau van de sector een risk assessment gebeurt. Ook voor de totaliteit van alle Belgische kmo's zou het nuttig zijn dat er een risk assessment zou gebeuren en dat er meer betrouwbare en gedetailleerde informatie zou bestaan over de cyberbedreigingen en de kosten daarvan.

De Hoge Raad vraagt dan ook dat de overheid het opstellen van sectorale risk assessments zou ondersteunen en er voor zorgt dat er meer betrouwbare data verzameld worden over de cyberbedreigingen voor de Belgische kmo's. Mede ook daarom dus de eerdere oproep in dit advies om te streven naar een betere dataverzameling en een gezamenlijke typologie voor cyberincidenten. Er is ook nood aan meer informatie over de efficiëntie en effectiviteit van acties en maatregelen, zowel op het niveau van de kmo als op beleidsniveau. In dat opzicht is het ook belangrijk op te volgen hoe andere landen het probleem van de cyberveiligheid van kmo's aanpakken. De rol die cyberverzekeringen voor kmo's kunnen spelen, vormt in dit kader een ander aandachtspunt.

7. Een beroeps- of sectorspecifieke benadering

De Hoge Raad is er van overtuigd dat de cyberveiligheid van kmo's best kan benaderd worden vanuit een beroeps- of sectorspecifieke benadering.

Ondernemingen binnen eenzelfde beroepssector lijken sterk op elkaar inzake soort activiteit, soorten gegevens, ondernemingsgrootte, ICT-omgeving en cyberveiligheidsmaturiteit. Ze zullen dus ook een vergelijkbaar risicoprofiel hebben en gelijkaardige behoeften inzake cyberbescherming. In plaats dat elke kmo individueel op zoek gaat naar oplossingen kunnen ze dat dus beter gezamenlijk doen binnen hun beroepssector.

Een beroeps- of sectorspecifieke benadering laat ook toe gebruik te maken van bestaande samenwerkingsstructuren en communicatiekanalen. In het bijzonder de beroepsorganisaties vormen een uitstekende partner voor de overheid en voor de kmo's om de kmo's te helpen hun cyberveiligheid te verhogen. Een beroepsorganisaties staat in rechtstreeks contact met heel wat kmo's uit de sector waarin ze actief is. Ze vormt een direct communicatiekanaal dat de ondernemers vertrouwen. Een beroepsorganisatie kent de beroepsactiviteiten en de ICT-omgeving waarbinnen de kmo's werken. Ook op het vlak van het ruimere digitaliseringsproces van de kmo is de beroepsorganisatie de aangewezen partner.

De Hoge Raad vraagt dan ook de overheid waar mogelijk voor een beroeps- of sectorspecifieke benadering kiest en beroeps- of sectorspecifieke initiatieven stimuleert en ondersteunt.

8. Cyberveiligheid als deel van digitalisering

Kmo's staan enerzijds voor de uitdaging hun cyberbescherming te verbeteren. Anderzijds staan ze voor de uitdaging van verdere digitalisering en digitale transformatie. Beide uitdagingen kunnen door de kmo best gezamenlijk en binnen het kader van hun beroepsorganisatie op sectorniveau worden aangegaan. In plaats van cyberveiligheid als een volledig afzonderlijke uitdaging te zien, kan deze gezien worden als een onderdeel van de digitalisering. Als men binnen een bepaalde sector of beroep bekijkt hoe de ideale digitale omgeving er voor een kmo binnen die sector of dat beroep uitziet en men deze probeert concreet vorm te geven, kan men tegelijkertijd nagaan hoe men daarbij voor voldoende cyberveiligheid kan zorgen.

Dit sluit bovendien aan bij het principe van security en privacy by design. In plaats van eerst een digitale omgeving uit te denken en te ontwikkelen en vervolgens na te denken over hoe men binnen die omgeving de cyberveiligheid kan waarborgen, kan de cyberveiligheid vanaf het begin meegenomen worden.

De Hoge Raad vraagt dan ook dat de overheid projecten binnen de beroepssectoren stimuleert en ondersteunt die concreet rond de digitalisering en cyberveiligheid van het beroep werken.

9. Cyberveiligheid is een primaire overheidstaak

Fysieke veiligheid wordt algemeen beschouwd als een basisrecht en de zorg ervoor als een primaire overheidstaak. Cyberveiligheid wordt echter vaak als een verantwoordelijkheid van de onderneming of als een gedeelde verantwoordelijkheid gezien. De nadruk die er in het kader van de algemene verordening gegevensbescherming op de verantwoordelijkheid van de onderneming wordt gelegd, heeft daar aan bijgedragen. De Hoge Raad erkent dat de kmo zelf een verantwoordelijkheid en rol dient op te nemen in het zich beschermen tegen cybercriminaliteit. De Hoge Raad en zijn leden ondernemen ook acties om de kmo's daar op te wijzen en hen daarbij te helpen. Dat neemt echter niet weg dat de zorg voor cyberveiligheid een primaire overheidstaak is en men de kmo in de eerste plaats moet zien als een (potentieel) slachtoffer.

De Hoge Raad vraagt dan ook dat overheid al het mogelijke doet om de cyberveiligheid van de kmo's te verbeteren, enerzijds door cybercriminaliteit aan te pakken en anderzijds door de cyberbescherming van de kmo's te helpen verhogen. De Hoge Raad vindt daarom de onderbestaffing van de Federal Computer Crime Unit (FCCU) van de federale politie onaanvaardbaar. Deze dienst zou net een van de speerpunten van het overheidsbeleid tegen cybercriminaliteit moeten vormen. Ook justitie moet van cybercriminaliteit een prioriteit maken. In het kader van de internationale samenwerking en diplomatie zou er moeten naar gestreefd worden dat derde landen de nodige acties ondernemen om cybercriminelen te identificeren en te bestraffen. Wat het Centrum voor Cyberveiligheid België (CCB) en het daartoe behorende Computer Emergency Response Team (CERT) betreft, vraagt de Hoge Raad dat deze diensten sterk zouden uitgebreid worden zodat alle ondernemingen hier voor hulp terecht kunnen en niet alleen de ondernemingen die kritische diensten leveren.

10. Nood aan beleidsafstemming

Bij cyberveiligheid zijn dus verschillende beleidsniveaus en tal van actoren betrokken. Voor de kmo's maakt het echter niet uit wie wat doet, als het maar gebeurt en als het maar goed gebeurt. De betrokkenheid van verschillende overheidsniveaus en overheidsactoren, is ook een positieve zaak aangezien er op deze manier veel middelen kunnen ingezet worden. Voorwaarde is wel een minimale afstemming en samenwerking. Indien verschillende overheidsniveaus, ministers en administraties vanuit hun eigen bevoegdheden een beleid voeren zonder dat op elkaar af te stemmen, zullen er problemen ontstaan zoals overlappingen, fragmentatie, tegenstellingen, verlaagde receptie door de doelgroep van het beleid, hiaten en gemiste synergiën. Kmo's hebben nood aan duidelijke, eenvoudige en eenduidige informatie. Voor hen wordt het net moeilijker als ze vanuit verschillende hoeken soortgelijke informatie en ondersteuning krijgen aangeboden. Tegelijkertijd zijn er nuttige acties die door geen enkele overheid worden uitgevoerd. Door samenwerking kunnen overheden elkaars acties ook versterken. Goede afstemming in alle fases van de beleidscyclus en tussen alle betrokken actoren is dus noodzakelijk.

De Hoge Raad stelt echter vast dat er momenteel heel weinig afstemming plaatsvindt:

- Momenteel is er nagenoeg geen strategische / beleidsmatige afstemming.
- Verschillende actoren werken aan soortgelijke cyberveiligheidsscans en assessment tools.

- Er bestaan verschillende informatieve gidsen en brochures die niet of weinig op elkaar zijn afgestemd.
- Overheden zijn niet op de hoogte van elkaars informatiecampagnes.
- Kmo's moeten cyberincidenten bij verschillende instanties melden.
- …

De Hoge Raad roept dan ook iedereen op meer in te zetten op een systematische, onderlinge afstemming en daarvoor gebruik te maken van de bestaande structuren of waar nodige daarvoor nieuwe structuren op te zetten.

11. Samenwerking promoten

Bij cyberveiligheid zijn tal van actoren betrokken. Samenwerking tussen die verschillende actoren zal zonder twijfel voor een beter resultaat zorgen. Kmo's kunnen via hun beroeps- en interprofessionele organisaties samenwerken. De ondernemersorganisaties kunnen op hun beurt met elkaar samenwerken. Daarnaast zijn er heel veel partnerschappen en synergiën mogelijk met andere overheids- en private actoren.

Om bijvoorbeeld informatie en instrumenten tot bij de kmo's te krijgen, kan er naast de ondernemers- en overheidsorganisaties ook met actoren gewerkt worden die een goed toegangskanaal tot de kmo's vormen en het vertrouwen van de kmo's genieten. Zowat alle kmo's zijn klant bij een telecomoperator, financiële instelling, verzekeraar, en vaak ook bij een boekhouder en ICT-dienstverlener. Door hun specifieke rol kunnen telecomoperatoren ook meer technische oplossingen tot bij de kmo's brengen. Wat de ICT-dienstverleners betreft, zouden er initiatieven moeten genomen worden om deze groep extra op te leiden op het vlak van cyberveiligheid. Op die manier kan de cyberveiligheid van de vele kmo's die beroep doen op externe ICT-ondersteuning verbeterd worden en wordt deels ook het probleem van de cyberveiligheids-'talent shortage' aangepakt.

Ook tal van interessante projecten die de cyberveiligheid van de kmo's ten goede komen (zoals bijvoorbeeld het opzetten van een phishing test platform voor kmo's, cyber security risk assessments per beroepssector, de evaluatie vanuit cyber security oogpunt van cloudoplossingen voor kmo's, …) zouden tot stand kunnen komen door samenwerking tussen kennisinstellingen, ondernemersorganisaties en overheid.

De Hoge Raad roept de beleidsverantwoordelijken dan ook op deze vormen van samenwerking te promoten en te ondersteunen. Zo kan men de rol van de Hoge Raad op het vlak van cyberveiligheid versterken door daar specifieke financiering voor te voorzien zodat de Hoge Raad meer tijd aan dit onderwerp kan besteden.

BESLUIT

Cybercriminaliteit vormt een steeds grotere bedreiging voor de kmo's. KMO-cyberveiligheid is dan ook een belangrijke beleidsprioriteit waar absoluut verder moet op ingezet worden. In dit advies heeft de Hoge Raad zijn visie op KMO-cyberveiligheid en op het daarop gerichte overheidsbeleid uiteengezet. Hij heeft de richtlijnen geformuleerd waarmee volgens hem het beleid dient rekening te houden en heeft daaraan voorstellen tot actie gekoppeld. Onderstaande tabel vat die richtlijnen en acties samen.

1. Een reëel probleem
- Kmo's blijvend informeren en sensibiliseren over het risico dat ze lopen - Campagne opbouwen rond getuigenissen van kmo's die slachtoffer werden - Meldingsbereidheid bij kmo's verhogen - Betere dataverzameling inzake cyberincidenten + gezamenlijke typologie
2. Overgrote meerderheid van de ondernemingen zijn kleine ondernemingen
- De kmo als uitgangspunt en norm nemen - Voldoende initiatieven nemen die zich specifiek op kmo's richten - Niet vergeten dat de meeste kmo's geen digitale of hoogtechnologische ondernemingen zijn - De groep van kmo's nog verder segmenteren
3. Specifieke situatie kmo's
- Voldoende en specifieke aandacht voor de kmo's hebben
4. Awareness en training op maat van de kmo's
- Pragmatische aanpak die focust op preventie, awareness en training en concrete gedragsverandering - Concrete en praktische informatie en instrumenten op maat van de kmo's - Informatie en instrumenten voor kmo's op één website groeperen - Voor acties die specifieke expertise vergen, overheidssteun voorzien + checklist dienstverlener - Voorzichtige benadering KMO-certificatie; certificatie van software en ICT-diensten wel goede piste
5. Zet in op technologische oplossingen
- Aanbod technologische oplossingen versterken, geschikt en toegankelijk maken en gebruik stimuleren - Er naar streven dat kmo's alleen maar veilige software gebruiken
6. Risk assessment voor aangepaste bescherming
- Sectorale risk assessments ondersteunen - Voor meer betrouwbare data over de cyberbedreigingen voor de Belgische kmo's zorgen - Efficiëntie en effectiviteit van acties en maatregelen op KMO- en op beleidsniveau onderzoeken - Aanpak andere landen vergelijken - Aandacht voor de rol van cyberverzekeringen
7. Een beroeps- of sectorspecifieke benadering
- Waar mogelijk voor een beroeps- of sectorspecifieke benadering kiezen - Beroeps- of sectorspecifieke initiatieven stimuleren en ondersteunen
8. Cyberveiligheid als deel van digitalisering
- Projecten rond digitalisering en cyberveiligheid binnen beroepssectoren stimuleren en ondersteunen

9. Cyberveiligheid is een primaire overheidstaak
- Cybercriminaliteit aanpakken, cyberbescherming helpen verhogen - De rol van FCCU, justitie, internationale samenwerking en diplomatie versterken - CCB/CERT versterken zodat ook alle kmo's daar met incidenten terecht kunnen
10. Nood aan beleidsafstemming
- Meer systematische, onderlinge afstemming d.m.v. bestaande of waar nodig nieuwe structuren
11. Samenwerking promoten
- Werk met trusted partners met toegang tot de kmo's - Initiatieven om de ICT-dienstverleners extra op te leiden op het vlak van cyberveiligheid - Samenwerking kennisinstellingen, ondernemersorganisaties en overheid stimuleren en ondersteunen - Versterk de rol van de HRZKMO op het vlak van cyberveiligheid