Consultatie Cyberveiligheidsbesluit

Auteur: Nigel van Houten
Datum: 17/3/2025

Inhoud:

Algemene overwegingen:

1. Volwassenheidsniveau doelgroep: de vereiste maatregelen zijn van dermate complexiteit dat de meeste MKB organisaties hier niet of nauwelijks aan kunnen voldoen. Naast de compliance belasting in uitvoering, bewijsvoering en handhaving/onderhoud vergt het ook een hoge mate van automatisering en implementatie van hulpmiddelen om aan de vereisten te voldoen. Aansluitend bij eerdere feedback door Omni-U - de benodigde volwassenheid is niveau 3-4 terwijl de meeste organisaties 0-1 hebben en 2 als ambitie hanteren.
2. Impliciete certificeringsplicht: een doorsnee ISO 27001 implementatie kost een organisatie doorgaans > €30.000,- aan directe en indirecte kosten. Hoewel er ook een impliciet terugverdienmodel in zit is de kans reëel dat startups en kleinere organisaties nooit meer onderdeel kunnen worden van een NIS2/CBB plichtige toeleveringsketen, aangezien de gehele keten moet voldoen aan de wet en niet alleen het bedrijf wat binnen de kaders van NIS2/CBB valt. Hoewel het CBB geen certificeringsplicht kent betekent dit mijn insziens automatisch dat bedrijven in hun toeleveringsketen terug gaan vallen op zo'n certificering: antwoord op de vraag of een ISO 27001 certificaat NIS2/CBB compliance impliceert is daarom zinvol maar ook hoe je als startup, zzp'er e.d. nog een kans maakt op de markt.
3. Focus op (bureaucratische) maatregelen ipv praktische verbeteringen: de bureaucratie rondom CBB levert in het beste geval een verbetering van de security binnen een organisatie op, terwijl alleen het daadwerkelijk praktisch pentesten/auditen van beveiligingsmaatregelen laat zien waar een bedrijf daadwerkelijk staat. De focus ligt echter op bureaucratie - de theoretische exercitie om tot een veiligere omgeving te komen. Voor organisaties die zich verslikken in het theoretische stuk is een pragmatische aanpak impactvoller omdat direct inzicht geeft in kwetsbaarheden en deze direct kan oplossen. Overweeg dus om dit om te draaien: start met een audit, verbeter en kijk daarna naar de theoretische kaders/redenen van

verbetering.Er is dan meteen een incentive tot handelen en opzet tot een GAP-analyse als basis. Geen beleidsstuk of procedure heeft ooit een hacker tegengehouden.

4. Overlap wetgeving en meldplichten: NIS2, DORA, AVG, CRA en anderen - in de basis vergen de meeste recente compliance eisen in grote lijnen hetzelfde van organisaties, alleen is de scope anders en is de invulling deels anders en gericht op de specifieke scope. Breng hier meer duidelijkheid in en werk met beslismodellen die leiden tot een overzicht van voor jou relevante maatregelen die genomen moeten worden en hoe dit zo effectief mogelijk gedaan kan worden. Idem met meldingsplicht(en): de potentieel ontstane fragmentatie en onduidelijkheid over wat, wanneer bij wie gemeld moet worden en wanneer gaat de implementatie en acceptatie enorm schaden en daardoor niet bijdragen bij het daadwerkelijk verbeteren van de beveiliging van bedrijven. Er is een duidelijke noodzaak tot implementatieondersteuning - de administratieve en bureaucratische belasting van implementatie van al deze wetgeving is simpelweg enorm.

Inhoudelijke reactie op het CBB

Artikel 6: Beveiliging bij het verwerven, ontwikkelen en onderhouden van netwerk- en informatiesystemen

- Artikel 6 vereist maatregelen voor de beveiliging bij het verwerven, ontwikkelen en onderhouden van netwerk- en informatiesystemen. De toelichting bij dit artikel zou specifieke aandacht kunnen besteden aan de beveiligingsaspecten in de verschillende fasen van de software development lifecycle (SDLC) en aan het belang van veilige configuraties en patchmanagement.
- Daarnaast zou het relevant zijn om te vermelden hoe organisaties de cybersecurityrisico's van externe softwareleveranciers en -ontwikkelaars kunnen beheersen, in lijn met de bredere focus op supply chain security.

Artikel 7: Beleid inzake risicoanalyse en beveiliging van informatiesystemen

- Artikel 7 vereist een beleid over risicoanalyse en beveiliging van informatiesystemen. Om de implementatie, met name voor het mkb, te vergemakkelijken, zou de toelichting bij dit artikel kunnen verwijzen naar concrete handreikingen, tools en sjablonen die de overheid ter beschikking stelt of die gangbaar zijn in de cybersecuritypraktijk. Het mkb-panel gaf bijvoorbeeld eerder aan het lastig te vinden om de risico's in hun netwerk- en informatiesystemen in te schatten.
- Daarnaast zou het nuttig zijn als de relatie tussen de vereiste risicoanalyse onder artikel 7 en de risicogebaseerde benadering die de NIS2-richtlijn en de Cyberbeveiligingswet hanteren, verder wordt geëxpliciteerd in de toelichting. Dit zou organisaties helpen om de scope en diepgang van hun risicoanalyses op een proportionele wijze te bepalen. Risicomanagement is immers een vak op zich.

Artikel 8: Incidentenbehandeling

- Artikel 8 schrijft voor dat het beleid voor incidentenbehandeling procedures moet bevatten voor diverse aspecten, waaronder detectie, analyse, reactie en herstel. Om onduidelijkheden te voorkomen, zou de toelichting bij dit artikel meer details kunnen bieden over de verwachte inhoud en het detailniveau van deze procedures. Hierbij kan verwezen worden naar *good practices* en standaarden op het gebied van incident management.
- Gezien de meldplicht voor significante incidenten binnen 24 uur na waarneming, zou artikel 8, of de toelichting hierop, kunnen benadrukken de noodzaak van procedures voor snelle detectie en initiële analyse van incidenten, zodat organisaties tijdig een vroege waarschuwing kunnen afgeven aan het CSIRT en de toezichthouder(s).

Artikel 9: Bedrijfscontinuïteit en crisisbeheer

- Artikel 9 behandelt bedrijfscontinuïteit, inclusief back-upbeheer en noodvoorzieningenplannen, en crisisbeheer. Het mkb-panel pleitte voor doelvoorschriften in plaats van gedetailleerde instructies, waarbij de precieze invulling aan de ondernemers wordt gelaten. De toelichting bij artikel 9 zou dit principe kunnen onderstrepen en voorbeelden kunnen geven van verschillende manieren waarop organisaties hun bedrijfscontinuïteit en crisisbeheer kunnen inrichten, afhankelijk van hun aard en omvang.
- Het zou tevens nuttig zijn als de toelichting op artikel 9 de relatie met eventuele bestaande bedrijfscontinuïteitsplannen (zoals die mogelijk al op grond van andere wet- en regelgeving bestaan) verduidelijkt, om onnodige dubbelingen te voorkomen. Zo vereisen Cybersecurity verzekeraars, Accountanskantoren en andere stakeholders ook steeds vaker aanvullende maatregelen of een Business Continuity Plan.

Artikel 10: Beveiliging van de toeleveringsketen

- Ten aanzien van artikel 6, dat de beveiligingsgerelateerde aspecten met betrekking tot de relaties tussen een organisatie en haar rechtstreekse leveranciers en dienstverleners adresseert, zou het nuttig zijn om meer concrete handvatten te bieden voor de inventarisatie en beoordeling van supply chain risico's, zeker gezien het feit dat dit als een grote uitdaging wordt beschouwd. Het zou waardevol zijn als de ministeriële regeling, waarnaar in de leeswijzer van het concept wordt verwezen, specifieke voorbeelden van gangbare cybersecuritypraktijken zou bevatten die organisaties kunnen volgen bij het uitvoeren van due diligence naar hun leveranciers. Hierbij zou ook rekening gehouden moeten worden met de verschillende soorten en groottes van organisaties, zoals de zorgen die door het mkb-panel zijn geuit over de haalbaarheid en betaalbaarheid van dergelijke maatregelen.
- Verder zou het verhelderend zijn als artikel 6 nadere invulling geeft aan wat er concreet wordt verwacht van de "beveiligingsgerelateerde aspecten" in de relatie met leveranciers. Duidelijkheid over de minimale eisen die gesteld worden aan

contractuele afspraken op het gebied van cybersecurity zou de implementatie ten goede komen. Het Digital Trust Center heeft gesprekken gevoerd met CISO's en ISO's over hun ervaringen met ketenbeveiliging en het bundelen van deze *good practices* in de toelichting op artikel 6 of in de ministeriële regeling zou zeer welkom zijn.

Artikel 11: Beleid en procedures voor het melden van significante incidenten

- Artikel 11 gaat over het beleid en de procedures voor het melden van significante incidenten. Zoals in de eerdere reactie is opgemerkt, is het cruciaal dat de criteria waaraan een incident moet voldoen om meldingsplichtig te zijn duidelijk en objectief zijn. De toelichting bij artikel 11 zou meer concrete voorbeelden en indicatoren kunnen geven van wat als een significant incident wordt beschouwd. Hierbij kunnen factoren zoals de impact op de dienstverlening, het aantal getroffen personen en de financiële schade worden genoemd.
- Verder zou de toelichting kunnen verduidelijken welke informatie minimaal vereist is in de vroege waarschuwing die binnen 24 uur na waarneming van het incident moet worden afgegeven. Ook de relatie met de meldplicht onder andere wetgeving, zoals de AVG of DORA, zou kort aangestipt kunnen worden om overlappingen en verwarring te minimaliseren. Het NCSC richt een centraal meldpunt in en het is belangrijk dat de procedures rondom deze meldingen helder zijn.

Algemene punten ter verbetering:

- Duidelijkheid voor het mkb: Zoals herhaaldelijk door het mkb-panel is benadrukt, is het van groot belang dat de eisen in het Cbb duidelijk, evenredig en proportioneel zijn, en dat er voldoende ondersteuning en handreikingen beschikbaar komen om de implementatie voor kleinere organisaties te vergemakkelijken. Het overwegen van de ISO27001-standaard als mogelijke kapstok, zoals gesuggereerd door het mkb, zou in de toelichting genoemd kunnen worden als een van de manieren om invulling te geven aan de vereisten.
- Implementatiegemak: Het Cbb zou, waar mogelijk, verwijzingen kunnen bevatten naar bestaande standaarden, *good practices* en hulpmiddelen die organisaties kunnen gebruiken bij de implementatie van de verschillende verplichtingen. Dit kan de drempel voor implementatie verlagen en de consistentie in de aanpak bevorderen. De vertraging in de implementatie benadrukt de complexiteit, en duidelijke, praktische richtlijnen zijn des te belangrijker.

Resumerend: behaalt de wet de gestelde doelen?

The good:

- Duidelijkheid en concretisering van de zorgplicht: Het Cbb beoogt de zorgplicht uit de Cyberbeveiligingswet (Cbw), die de NIS2-richtlijn implementeert, nader uit te werken. Door in ministeriële regelingen sectorale invulling van de zorgplicht mogelijk te maken, kan beter worden ingespeeld op de specifieke aard en risico's van verschillende sectoren, subsectoren en soorten entiteiten. Dit maatwerk kan de effectiviteit van de beveiligingsmaatregelen vergroten.
- Focus op risicomanagement: Het Cbb benadrukt het belang van risicoanalyses en beveiligingsbeleid. Essentiële en belangrijke entiteiten moeten beleid opstellen voor risicoanalyse en de beveiliging van hun netwerk- en informatiesystemen. Dit fundamentele principe van cybersecurity is cruciaal voor het identificeren en mitigeren van bedreigingen. Echter: een goed beleid heeft nog nooit een hacker tegengehouden om een systeem binnen te dringen - audit/pentest is dus essentieel om beleid te valideren. Overweeg het daarom om te draaien en te starten met een pentest/audit.
- Aanstelling van CSIRT's en een coördinator voor kwetsbaarheden: Het Cbb regelt de aanwijzing van Computer Security Incident Response Teams (CSIRT's) en een coördinator voor de gecoördineerde bekendmaking van kwetsbaarheden. Deze structuren zijn essentieel voor het vroegtijdig waarschuwen bij dreigingen, het verlenen van bijstand bij incidenten en het verbeteren van de algehele cyberweerbaarheid. Het Nationale Cyber Security Centrum (NCSC) zal in de praktijk een belangrijke rol spelen als CSIRT en coördinator.
- Verplichtingen voor bestuurders: Het Cbb stelt opleidingseisen aan bestuurders van essentiële en belangrijke entiteiten. Zij moeten beschikken over voldoende kennis en vaardigheden om risico's te identificeren en risicobeheersmaatregelen te beoordelen. Dit verhoogt het bewustzijn en de verantwoordelijkheid op het hoogste niveau van de organisatie. Keerzijde zijn kosten en haalbaarheid: waar houdt de (inhoudelijke) kennis vereiste voor een bestuurder op.
- Bevordering van informatie-uitwisseling: Hoewel niet expliciet een direct doel van het Cbb zelf, faciliteert de onderliggende NIS2-richtlijn en de Cbw de informatie-uitwisseling over dreigingen en kwetsbaarheden. Dit collectieve aspect kan de algehele beveiliging verbeteren.

The bad:

- Lasten voor het MKB: Zoals in de nota van toelichting wordt erkend, kunnen de nalevingskosten en -lasten voor het midden- en kleinbedrijf (mkb) een significante uitdaging vormen. Er is bezorgdheid geuit over de haalbaarheid en betaalbaarheid van de vereisten, de complexiteit van de regelgeving en de noodzaak van duidelijke richtlijnen en ondersteuning voor kmo's. Als de Cbb niet voldoende rekening houdt

met de specifieke omstandigheden van mkb-bedrijven, kan dit de effectieve implementatie belemmeren.

- Vage of brede formuleringen: Het mkb-panel heeft gepleit voor duidelijkheid over het toepassingsbereik en de betekenis van specifieke begrippen. Indien de ministeriële regelingen en het Cbb zelf te algemeen of onduidelijk zijn geformuleerd, kan dit leiden tot interpretatieverschillen en een inconsistente implementatie.
- Focus op administratie in plaats van daadwerkelijke maatregelen: Er is een risico dat de nadruk te veel komt te liggen op administratieve verplichtingen (zoals documentatie en registratie) ten koste van de daadwerkelijke implementatie van beveiligingsmaatregelen. Dit zou de beoogde verbetering van de cyberweerbaarheid kunnen ondermijnen en komt terug bij de suggestie om de focus te leggen op daadwerkelijke praktische beveiligingschecks.
- Afhankelijkheid van sectorale ministeriële regelingen: De effectiviteit van het Cbb is sterk afhankelijk van de kwaliteit en tijdigheid van de ministeriële regelingen die de zorgplicht per sector verder invullen. Indien deze regelingen te laat komen, onvoldoende specifiek zijn of inconsistenties vertonen, kan dit de beoogde harmonisatie en effectiviteit van de cyber security maatregelen schaden.
- Complexiteit van de toeleveringsketen: Het beveiligen van de toeleveringsketen wordt als een grote uitdaging beschouwd. Kleine toeleveranciers kunnen moeite hebben om aan de eisen te voldoen. Zonder effectieve mechanismen om ook de cybersecurity in de bredere toeleveringsketen te waarborgen, blijven organisaties kwetsbaar. Daarbij kan het bedrijven buitensluiten op de markt en hun levensvatbaarheid bedreigen.

Concluderend:

Het Cbb heeft potentie om de cyberbeveiliging in Nederland te verbeteren door de zorgplicht te concretiseren, risicomanagement te benadrukken, structuren te creëren voor incidentrespons, audits en pentests de feitelijke situatie laten beoordelen en bestuurders meer verantwoordelijk te maken. Het succes ervan zal in grote mate afhangen van de mate waarin rekening wordt gehouden met de uitdagingen voor het mkb, de duidelijkheid van de regelgeving, de focus op daadwerkelijke beveiligingsmaatregelen en de effectieve uitwerking van de sectorale ministeriële regelingen. Daarnaast is een adequate aanpak van de beveiliging van de toeleveringsketen essentieel. Zonder deze elementen kan het Cbb mogelijk niet volledig zijn beoogde doel bereiken.

Bijlage: administratieve belasting

Hieronder een opsomming van de gevonden (administratieve) plichten binnen het CBB:

- Het opstellen van een beleid waarin afhankelijkheidsrelaties met directe leveranciers en dienstverleners in kaart worden gebracht.
- Het opstellen van een beleid dat gericht is op de IT-toeleveringsketen.
- Het maken van goede afspraken om zicht te houden op de risico's in de toeleveringsketen en deze indien nodig te beperken.
- Het periodiek uitvoeren van kwetsbaarheidsscans (waar passend) en het vastleggen van de resultaten.
- Het nemen van maatregelen om potentiële kwetsbaarheden aan te pakken.
- Indien potentiële gevolgen van kwetsbaarheden dit rechtvaardigen, het opstellen en uitvoeren van een plan om de desbetreffende kwetsbaarheden te beperken.
- In alle overige gevallen, het naar behoren motiveren en documenteren van het niet nemen van maatregelen tegen kwetsbaarheden.
- Evenals bij het niet toepassen van een beveiligingspatch, het motiveren en documenteren waarom van een wettelijke verplichting wordt afgeweken.
- Het schriftelijk vaststellen en aantoonbaar toepassen van beleid over verschillende onderwerpen (nader uitgewerkt in ministeriële regelingen).
- Registratie bij het Nationaal Cyber Security Centrum (NCSC) in het entiteitenregister.
- Het aanleveren van gegevens voor het entiteitenregister, zoals contactgegevens en de sector(en) waarin de organisatie actief is.
- Het melden van significante incidenten onverwijld (en indien niet mogelijk, binnen 24 uur) bij het CSIRT en de toezichthouder.
- Binnen 72 uur na melding van een significant incident, het indienen van een rapportage met de initiële beoordeling, ernst, gevolgen en (indien mogelijk) signalen van aantasting.
- Het goedkeuren van de genomen beveiligingsmaatregelen door het bestuur.
- Toezicht houden op de uitvoering van de beveiligingsmaatregelen door het bestuur.
- Het volgen van een opleiding door de leden van het bestuur om risico’s te kunnen identificeren en risicobeheersmaatregelen te kunnen beoordelen.
- Het periodiek evalueren en herzien van het beleid voor de toeleveringsketen (impliciet in het opstellen van een beleidsplan).
- Het ontwikkelen en testen van bedrijfscontinuïteits- en herstelplannen (documentatie hiervan is impliciet).
- Het regelmatig uitvoeren van risicobeoordelingen.
- Het implementeren van passende beveiligingsmaatregelen op basis van de risicobeoordeling.
- Het opstellen van een beleidsplan voor de toeleveringsketen.
- Het in kaart brengen van rechtstreekse leveranciers.
- Het bepalen van de meest relevante risico's.