Deloitte Risk Advisory B.V.
Gustav Mahlerlaan 2970
1081 LA Amsterdam
Postbus 58110
1040 HC Amsterdam
Nederland

Tel: 088 288 2888
Fax: 088 288 9711
www.deloitte.nl

Aan: Ministerie van Justitie en Veiligheid

Datum
23 augustus 2021

Onderwerp
Betreft internetconsultatie Wijziging Wet beveiliging netwerk- en informatiesystemen i.v.m. uitbreiding bevoegdheid MinJenV

U heeft een wijziging op de Wet beveiliging netwerk- en informatiesystemen (Wbni) voorgelegd voor een internetconsultatie. Deloitte Risk Advisory B.V. (hierna "Deloitte") wil u graag enkele aandachtspunten meegeven.

Belang van een weerbaar Nederland

Elke denkbare sector in Nederland is in hoog tempo aan het digitaliseren. Als gevolg daarvan zien we bij Deloitte dat criminelen hier misbruik van maken en cybercriminaliteit met de dag geavanceerder wordt, meer impact heeft en in volume exponentieel toeneemt. De steeds beter georganiseerde cybercriminelen vergen van elk bedrijf in Nederland, groot en klein, dat zij haar informatiesystemen adequaat beveiligt. Tegelijk is echter een trend zichtbaar waarbij de steeds complexere, en voor bedrijfsvoering cruciale informatiesystemen lastig te beveiligen zijn, en waarbij uitval enorme gevolgen voor de continuïteit van organisaties kan hebben. Het is daarom onder andere van belang dat organisaties doorlopend worden voorzien van actuele informatie die hen kan helpen om de volgende grote aanval voor te zijn of af te wenden.

Daarom erkennen wij het belang en vooral ook de *urgentie* van de voorgestelde wetswijziging op de Wbni, om de informatiestroom vanuit het NCSC uit te breiden van alleen vitale aanbieders naar ook *andere aanbieders*. Op dit moment ontbreekt een dergelijke structurele informatiestroom omdat het NCSC uitsluitend een aangewezen groep vitale organisaties kan en mag bijstaan en voorzien van informatie.

Het is te kort door de bocht om te denken dat we onze vitale sectoren (voor zover die überhaupt echt af te bakenen zijn als zodanig) kunnen helpen door alleen hen, en niet ook hun leveranciers, partners en afnemers te beschouwen. Vanuit ons dagelijks werk zien wij de risico's en enorme impact die cyberaanvallen op derde partijen kunnen hebben op de bedrijven waar zij zaken mee doen en diensten aan leveren. Daarom kunnen deze andere aanbieders in sommige gevallen even vitaal voor onze maatschappij zijn als een aanbieder van vitale diensten zelf.

Kortom, wij pleiten van harte voor wetgeving die maakt dat informatiestromen richting een veel bredere groep bedrijven structureel mogelijk maakt.

Wij hebben daarbij nog wel een aantal aandachtspunten die wij graag willen communiceren middels deze internetconsultatie:

Haast is geboden

Het is van het grootste belang voor de weerbaarheid van onze (digitale) samenleving dat er snel uitgebreidere mogelijkheden komen om vanuit de overheid dreigingsinformatie rondom cyberactoren, -aanvallen en -kwetsbaarheden sneller, breder en meer gestructureerd te kunnen delen met partijen die daar direct actie op kunnen nemen. Het is in onze ogen onbestaanbaar dat een modern en gedigitaliseerd land als Nederland haar

tanden anno 2021 nog stuk bijt op juridische obstakels die niemand lijken te dienen maar informatiedeling wel aanzienlijk hinderen. Het is goed om te zien dat met deze wetswijziging een aantal broodnodige veranderingen worden ingezet, die zullen maken dat zowel publiek als privaat in de toekomst een sterkere en bredere bijdrage kunnen leveren aan de (digitale) veiligheid van onze samenleving.

Informatie delen enkel voor bijzondere gevallen

Het voorstel geeft aan dat er enkel in "bijzondere gevallen" zogenoemde *restdata* gedeeld wordt naar andere aanbieders door het NCSC of middels schakelorganisaties. Uit de toelichting valt op te maken dat op basis van de noodzakelijkheidstoets van de AVG door het NCSC wordt bepaald of informatie delen noodzakelijk (o.a. proportioneel) is. Oftewel: Het NCSC moet, alvorens zij informatie mag delen, kunnen bepalen of een dreiging of incident potentieel aanzienlijke gevolgen voor de continuïteit van de dienstverlening van een aanbieder kan hebben.

Wij verwachten dat het NCSC dit vaak niet zal kunnen bepalen, of dat veel werk komt kijken bij het uitvoeren van een dergelijke toets (zeker wanneer dit op grote schaal nodig is). Een bepaalde kwetsbaarheid of dreiging kan een impact hebben op een specifieke set van systemen bij een organisatie. Dit is echter informatie die het NCSC niet per se bezit over een aanbieder (vitaal of anderszins). Daarom verwachten wij dat het NCSC niet in alle gevallen voldoende (snel) kan beoordelen of het delen van informatie proportioneel is. Het gevolg zou dan zijn dat informatie alsnog niet gedeeld kan worden, waardoor een grote kans bestaat dat de wet in haar huidige voorgestelde vorm onvoldoende verbetering biedt ten opzichte van de huidige situatie.

Daarom pleiten wij ervoor dat het delen van restdata met andere aanbieders via het NCSC of een schakelorganisatie de norm zou moeten worden, tenzij duidelijk is dat hier grote bezwaren tegen bestaan ("delen tenzij"). Op deze manier gaat geen kostbare tijd verloren aan het vaststellen of sprake is van een bijzonder geval en kan informatie zonder onnodige beperkingen breed gedeeld worden. Ten slotte kan (zoals o.a. het NCSC nu al doet) aan de hand van publieke standaarden[1] bepaald worden of kwetsbaarheden een hoge dreiging kunnen vormen voor een organisatie en op basis daarvan met extra urgentie informatie gedeeld worden. Als dan toch een zekere toets ingebouwd moet worden zou in onze ogen, gezien de snelheid van handelen die noodzakelijk is, gebruik van een dergelijke score een passender middel zijn om de proportionaliteit vast te stellen dan een gedetailleerde inhoudelijke analyse.

Het belang van één loket

In een recent door ons uitgevoerd benchmarkonderzoek naar de governance en cyberweerbaarheidsinitiatieven in een zestal andere landen[2] (met vergelijkbare digitaliseringsgraad als Nederland) komt duidelijk naar voren dat Nederland één van de weinige landen is waar de overheid haar activiteiten op cyberweerbaarheid niet centraal op één plek heeft belegd. Het is vanuit het perspectief van bedrijven en burgers in sommige gevallen erg onduidelijk waar zij al dan niet terecht kunnen met vragen, voor advies en voor het verkrijgen van dreigingsinformatie (voor dat laatste op dit moment in de meeste gevallen nog helemaal nergens). Daarnaast speelt het bestaan van meerdere "loketten" natuurlijk

---

[1] Zie *Common Vulnerability Scoring System* (CVSS) Scores, https://www.first.org/cvss/

[2] Zie de bijlage bij het Cyber Security Raad rapport "Integrale aanpak cyberweerbaarheid" waar Deloitte de benchmark voor heeft uitgevoerd: https://www.cybersecurityraad.nl/documenten/adviezen/2021/04/06/csr-adviesrapport-integrale-aanpak-cyberweerbaarheid

misverstanden, inefficiënte communicatie en vertragingen tijdens grote cyberincidenten in de hand. In het licht van deze consultatie en de gelijktijdig lopende consultatie voor de Wet bevordering digitale weerbaarheid van bedrijven (vanuit het Ministerie van Economische Zaken en Klimaat), zou het in onze ogen voor de hand liggend zijn dat niet alleen de juridische obstakels voor het delen van informatie worden weggenomen maar nu ook snel een voorstel wordt gedaan voor een centraal loket voor overheden, bedrijven en burgers die dient als "one stop shop" voor cyber-gerelateerde vraagstukken, informatie en advies. Een dergelijk loket is een belangrijk instrument in het snel en efficiënt delen van dreigingsinformatie en zou daarom een zeer welkome aanvulling zijn in het Nederlandse cyberlandschap. Wij kunnen ons voorstellen dat het niet binnen de reikwijdte van deze wetswijziging valt, maar het is desondanks goed om alvast na te denken over een goede en efficiënte uitvoering van de informatiedeling in de toekomst

Deloitte hoopt u met deze brief voldoende te hebben geïnformeerd en te hebben voorzien van een waardevolle bijdrage in het verder verfijnen van het wetsvoorstel. Mocht u nog nadere vragen hebben, dan kunt u contact opnemen met Kevin Jonkers, Director Cyber Security op 06-30313023 of via kejonkers@deloitte.nl

Met vriendelijke groet,

Kevin Jonkers

Deloitte Risk Advisory B.V.