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 Wet bevordering digitale weerbaarheid bedrijven

U heeft de Wet bevordering digitale weerbaarheid bedrijven voorgelegd voor een internetconsultatie. Deloitte Risk Advisory 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 van deze wet om de digitale weerbaarheid van alle Nederlandse bedrijven te verhogen, ook die bedrijven die nu of in de toekomst niet als vitaal zijn aangemerkt. In ons dagelijks werk identificeren wij dezelfde uitdagingen in kleine en grote bedrijven om a) informatiebeveiliging toegankelijk te maken en b) weloverwogen en op data gebaseerde beslissingen te maken over welke maatregelen een bedrijf moet treffen. Daarom moedigen wij het delen van dreigingsinformatie en de ontwikkeling van praktische handvatten voor het bedrijfsleven toe.

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:

Data-analyse van dreigingsinformatie niet optimaal ingericht

In het wetsvoorstel wordt aangegeven dat de Minister ook specifieke dreigingsinformatie kan uitwisselen met het niet-vitale bedrijfsleven. Dit is een ontwikkeling die wij toejuichen en aanmoedigen. Wij zijn overtuigd dat betere informatie-uitwisseling kan leiden tot betere en tijdige inzichten over het dreigingslandschap. Echter, wij identificeren ook enige overlap in de activiteiten van het NCSC en het DTC. Waarbij beide partijen kans lopen om aparte analyses uit te voeren over dezelfde data of zelfs tot dezelfde inzichten te komen. Dit is niet optimaal. Wij raden daarom aan om te kijken of het niet mogelijk is dat het DTC een afnemer wordt van het NCSC en hun zogenoemde *restdata*. De rol van het DTC kan die van communicatie en interpretatie van technische dreigingsinformatie zijn en dit begrijpelijk maken voor het gemiddelde Nederlandse bedrijf. Tevens kan dit voorkomen dat er dubbele waarschuwingen worden gedeeld vanuit het NCSC en de DTC.

Beveiliging van gedeelde gegevens

In artikel vier, eerste lid geeft u aan dat de Minister dreigingsinformatie uit kan wisselen mits hij acht dat de gegevens gebruikt zullen worden voor het beoogde doel en de beveiliging van het bedrijf op orde is. Momenteel is niet nader toegelicht of en hoe de Minister dit zal toetsen bij desbetreffende bedrijven. Het delen van gevoelige dreigingsinformatie met bedrijven die onvoldoende hun beveiliging op orde hebben kan datalekken van bedrijfsgevoelige en privacygevoelige informatie in het ergste geval juist verder in de hand werken. Daarom raden wij aan te specifiëren dat de Minister een best-practice norm voor informatiebeveiliging of een ander toetsingskader aanhaalt om te bepalen of een bedrijfsgevoelige informatie mag ontvangen. Daarbij is differentiatie op gevoeligheid noodzakelijk, zodat minder gevoelige informatie eventueel breder gedeeld kan worden dan bijvoorbeeld zeer specifieke en extra gevoelige informatie.

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.