Reactie op internetconsultatie voorstel aanpassing Wet beveiliging netwerk- en informatiesystemen

Onderwerp;	Wet beveiliging netwerk- en informatiesystemen
Afkomstig van;	VNO-NCW/MKB-Nederland
Datum;	Augustus 2021
Inlichtingen;	mevr. mr. N. Mallens/ mallens@vnoncw-mkb.nl

Graag maken VNO-NCW en MKB-Nederland gebruik van de mogelijkheid te reageren op het concept voorstel tot wijziging van de Wet beveiliging netwerk- en informatiesystemen (Wbni).

Met dit voorstel wordt expliciet mogelijk gemaakt dat het NCSC in ruimere mate dreigings- en incidentinformatie mag delen buiten de doelgroep. Ook organisaties die objectief kenbaar tot taak hebben om andere organisaties of het publiek daarover te informeren (OKTT's) krijgen voortaan deze informatie van het NCSC, waarop zij, op hun beurt, hun achterbannen kunnen informeren.

VNO-NCW en MKB-Nederland juichen deze aanpassing van de Wbni toe. Wij pleiten al langere tijd voor betere en veel bredere informatiedeling ten behoeve van de digitale veiligheid. Ook bedrijven die niet tot de vitale infrastructuur behoren moeten worden voorzien van goede informatie. Buiten de vitale infrastructuur spelen immers eveneens grote belangen die bescherming verdienen. Namelijk het belang van ondernemers én werknemers om grote schade aan ondernemingen te voorkomen, het belang van continuïteit van dienstverlening in de keten, en de doorwerking van dat alles in de macro-economie, de verdiencapaciteit en de brede welvaart.
Naast algemene informatie zijn met name specifieke, gerichte waarschuwingen over kwetsbare of gecompromitteerde systemen cruciaal voor alle bedrijven om maatregelen te nemen ter versterking van de cyberweerbaarheid.

Het wetsvoorstel creëert daarnaast, met de wijziging van artikel 3, ook een grondslag voor het NCSC om in bijzondere gevallen zelf rechtstreeks informatie te delen, zonder tussenkomst van schakelorganisaties. Dit is het geval als er geen specifieke schakelorganisatie is én het informatie over een dreiging of incident betreft met (potentieel) aanzienlijke gevolgen voor de continuïteit van de dienstverlening van de betrokken aanbieder.

Dit laatste laat de nodige interpretatieruimte bij het NCSC over wanneer sprake is van aanzienlijke gevolgen voor de continuïteit.
Wij vragen ons af of het NCSC deze beoordeling in alle gevallen wel kan maken aangezien het bedrijven betreft die niet tot de doelgroep van het NCSC behoren. Wij vinden dat in ieder geval moet worden voorkomen dat er een té restrictieve interpretatie van de regelgeving gaat ontstaan.

Het uitgangspunt moet zijn dat de drempels voor het delen van informatie door het NCSC met organisaties die niet tot zijn doelgroep behoren zo laag mogelijk worden gehouden om schade te voorkomen en met het oog op de brede belang van digitale veiligheid. Snellere en ruimhartige deling van relevante informatie is niet alleen van belang voor de continuïteit van de dienstverlening, maar ook om grote schadeposten voor ondernemers en ondernemingen, en daarmee in potentie voor de economie als geheel, te voorkomen.

Tot slot dringen wij erop aan om, in afwachting van de wijziging van de Wbni, nu al tot het delen van incidentinformatie met OKTT's over te gaan. Het is lastig uitlegbaar dat bedrijven schade oplopen als gevolg van cybercriminaliteit die had kunnen worden voorkomen als de informatie door de overheid zou zijn gedeeld. Helaas is dat op dit moment met de huidige interpretatie van de wettelijke bepalingen niet uit te sluiten en dat is ronduit zorgelijk.