Hoogerheide, 29 juni 2024

Betreft: Reactie internetconsultatie Cyberbeveiligingswet

Geachte heer/mevrouw,

Hierbij de reactie van Matthijs BV op de internetconsultatie van de Cyberbeveiligingswet.

Het doel van de wet en de bewustwording van de gevaren m.b.t. digitale systemen ondersteunen we als Matthijs BV. Desondanks hebben wij op de volgende punten nog vragen en/of opmerkingen.

Hoofdstuk 8 Governance

Artikel 26 stelt verschillende eisen aan de kennis en vaardigheden van het bestuur van een essentiële- of belangrijke entiteit. Dit artikel werkt onnodig verzwarend voor het MKB. De “cyber omgeving” is constant in beweging en heel dynamisch, zo ook met betrekking tot dreigingen en beveiligingen. Waarom is het niet voldoende om toegewijd en geschoold personeel in dienst te hebben op dit vlak?

Hoofdstuk 9
§ 9.1 Meldplicht

De huidige opgestelde serie aan stappen onder de meldplicht is onnodig zwaar vanuit het perspectief van een middelgrote belangrijke entiteit.

Het is voor een belangrijke entiteit beter werkbaar om artikel 28 (vroegtijdige waarschuwing) te schrappen en artikel 29 aan te passen naar 48 uur in plaats van 72 uur.

Het tussentijds verslag zoals deze beschreven is in artikel 30 is onduidelijk. Onder welke voorwaarden doet het CSIRT het verzoek om een tussentijds verslag op te stellen? Wat wordt verstaan onder een “verslag”? Is deze stap niet overbodig? Binnen één maand moet een entiteit een eindverslag indienen en anders een voortgangsverslag, mits het incident voortduurt. De huidige regeldruk is al hoog en deze verschillende stappen en verslagen zijn niet genoeg gestroomlijnd, het is opgesteld vanuit het perspectief van de overheid niet vanuit het werkveld.

Aangezien een onderneming naast de bevoegde autoriteit en de CSIRT ook nog een verplichte toezichthouder krijgt. Kan deze toezichthouder, die ook bijstand kan verlenen ten tijde van een incident, niet de centrale plek zijn om de melding te doen? Zodat de onderneming maar bij één iemand moet/kan melden en niet ook nog apart de autoriteit of CSIRT op de hoogte hoeft te stellen.

Hoofdstuk 16
§ 16.3 Handhaving ten aanzien van belangrijke entiteiten

De kosten van de beveiligingsscan (artikel 79) door een onafhankelijke partij horen niet gedragen te worden door de belangrijke entiteit zelf. De overheid stelt de wet op, de overheid handhaaft en kosten gemoeid met de handhaving en controles zouden voor ook voor de overheid moeten zijn.

Artikel 80 de verplichting om een gerichte beveiligingsscan uit te voeren is buitenproportioneel voor een niet essentiële maar belangrijke entiteit. Artikel 80 lid 4, de kosten van de gerichte beveiligingsscan horen niet gedragen te worden door de belangrijke entiteit zelf.

Het openbaar maken van een overtreding zoals deze beschreven is in artikel 81 is onduidelijk en te breed. Het openbaar maken “op een door de bevoegde autoriteit bepaalde wijze” kan dus variëren per autoriteit en contactpersoon. Kan de wijze van openbaar maken gespecificeerd worden? Zo weten de entiteiten waar ze aan toe zijn.

Met vriendelijke groet,
QHSE Coördinator Matthijs BV