Onze nationale, digitale veiligheid: van compliance naar risicobeheersing

Hoe kan de WBNI de digitale veiligheid van onze voornaamste infrastructuur versterken?

Highlights

- De WBNI is de Nederlandse vertaalslag van de Europese Netwerk- en Informatiebeveiligingsrichtlijn.
- Aanbieders van essentiële diensten moeten cyberbeveiliging in hun risicocultuur integreren.
- De wet is een unieke kans om op bestuursniveau aandacht te krijgen voor cybersecurity.
- De implementatie zal worden gecontroleerd door de publieke autoriteiten.
- Publiek-private samenwerking is essentieel voor een duurzame naleving.

Anders dan een cyclische compliance-benadering van cyberveiligheid, triggert de WBNI een nieuwe visie door een risicobeheercultuur op alle lagen te bevorderen.

Het is al vaak besproken dat onze samenleving steeds afhankelijker wordt van digitale systemen en infrastructuur. Toenemende digitale dreigingen en belangen worden door het NCSC jaarlijks beschreven in het Cybersecuritybeeld Nederland. De WRR concludeerde al in 2019 dat toenemende risico's de overheid ertoe dwingen om een grotere rol te spelen in de digitale veiligheid van onze kritieke infrastructuur. Met de invoering van de WBNI is deze rol voor het eerst vastgelegd in wet- en regelgeving.

Met de focus op het creëren van een 'risico-managementcultuur', vereist de WBNI dat organisaties in de vitale infrastructuur een minimum niveau van digitale beveiliging borgen. De continuïteit van bijvoorbeeld onze havenbedrijven is immers niet alleen in het belang van deze (commerciële) organisaties, maar in het belang van ons allemaal. Wat zou er in de samenleving gebeuren als er enkele weken slechts beperkte import van voedsel, brandstof of grondstoffen mogelijk zou zijn?

Daarbij krijgt de private sector de verantwoordelijkheid om hun kernprocessen te beveiligen als die van belang zijn voor nationale stabiliteit, weerbaarheid en economie.

Het succes van de WBNI wordt echter mede bepaald door de opstelling van private organisaties én de overheid. Het risico bestaat dat private organisaties de WBNI beschouwen als een compliance oefening in plaats van een actiegerichte oproep om de security-volwassenheid te vergroten. De vraag is dan ook, hoe we ervoor kunnen zorgen dat de WBNI de drijvende kracht wordt om de security-volwassenheid te versnellen binnen de nationale kritieke infrastructuur?

Cybersecurity als onderdeel van de risicocultuur van de organisatie

De EU heeft in 2016 de Network and Information Systems (NIS) Directive aangenomen om de kritieke infrastructuur te beschermen en de samenwerking rondom incident meldingen te versnellen. De NIS Directive is in Nederland in 2018 omgedoopt tot de Wet beveiliging netwerk- en informatiesystemen (WBNI). Met de invoering van de WBNI ontstaat er voor het eerst een wettelijke verplichting voor een aantal belangrijke organisaties/bedrijven die cruciale diensten leveren voor het functioneren van onze maatschappij om 'passende technische en organisatorische' maatregelen te nemen om de digitale veiligheid te borgen. Bijvoorbeeld door gebruik van encryptie, awareness campagnes en security- monitoring.

Het principe is natuurlijk niet nieuw. Veel bedrijven baseren hun informatiebeveiligingsbeleid al jaren op (internationale) standaarden, zoals ISO 27001 of NIST. Dergelijke standaarden stellen eigenlijk allemaal dat het bedrijf maatregelen moet implementeren om de geïdentificeerde risico's te beheersen

tot een acceptabel niveau. Tot zo ver lijkt de WBNI dus logisch aan te sluiten op de bekende werkwijze van de meeste organisaties. Dat was overigens ook de bedoeling van de wetgever. Een en ander zou de indruk kunnen wekken dat organisaties weinig hoeven te doen om voorbereid te zijn op de WBNI. Dat zou echter een misrekening zijn die niet alleen kan leiden tot onderschatting van de compliance-vereisten, maar belangrijker nog tot ondermijning van de effectiviteit van de WBNI om de Nederlandse samenleving te beschermen. De risicoanalyses moeten namelijk vooral ook rekening houden met impact op de samenleving en niet alleen met de impact op het bedrijf. Het is de vraag of de vitale bedrijven hier voldoende aandacht aan geven.

De vergelijking naar een enigszins gerelateerde wetgeving is interessant. Daar waar de maatschappelijke aandacht voor de WBNI vooralsnog vrij beperkt blijft, leidde de Algemene Verordening Gegevensbescherming (AVG) tot veel beroering. Dat is opmerkelijk, ook de WBNI kent de bevoegde autoriteit immers de mogelijkheid toe om een stevige bestuurlijke boete van maximaal 5 miljoen euro op te leggen. Dat is weliswaar minder dan de maximale boete onder de AVG, maar desondanks nog altijd een stevig bedrag. Het ontbreken van publieke aandacht kan ook juist een positieve bijdrage leveren aan de implementatie van de WBNI. Een paniekerige respons leidt al snel tot windowdressing en compliance-denken en vaak te weinig tot inhoudelijke actie om de digitale veiligheid te versterken.

Tegelijkertijd moeten vitale organisaties en digitale dienstverleners zich niet in slaap laten sussen. De publieke aandacht, meldplicht van incidenten, toezichthoudende rol van de overheid en juridische context gaan zorgen voor een nieuwe dynamiek in de organisatie. Door de WBNI als wetgevend kader zullen bestuurders zich moeten realiseren dat cyberveiligheid direct raakt aan de bedrijfsvoering, het vertrouwen van klanten en de stabiliteit van de samenleving. De WBNI zou door bedrijven in onze vitale infrastructuur dus niet alleen moeten worden benaderd als een gangbare 'checkbox-compliance' maar als een unieke kans om hun algehele benadering van cyberveiligheid opnieuw vorm te geven. Dit is ook in lijn met de ENISA-richtlijnen die de volledige cybersecurity-lifecycle bestrijken – van governance en bedrijfscontinuïteit tot detectie en respons. Gelukkig zien wij dat bedrijven zich steeds meer realiseren dat zij in de weerbaarheid van hun cyberveiligheid blijvend moeten versterken.

Het is daarbij interessant dat de WBNI belicht dat cybersecurity niet beschouwd moet worden als een IT-kwestie, maar als een integraal onderdeel van de kritieke operatie en strategische besluitvorming. Op dit moment wordt cyberveiligheid nog te vaak gezien als een verantwoordelijkheid van de IT-afdeling. De invoering van de WBNI maakt het glashelder dat dit onderwerp aandacht verdient op het hoogste bestuurlijke niveau. Wat ons betreft met één kapitein, bij voorkeur de CISO, die stuurt op de digitale veiligheid en belangrijke zaken adresseert in direct overleg met het bestuur, de juridische en compliance-afdelingen én de business. Het is cruciaal dat belangrijke stakeholders binnen organisaties snel gezamenlijk bepalen hoe ze dit zo goed mogelijk organiseren.

Samenwerking met partijen in een veranderend speelveld

In de afgelopen jaren is cyberveiligheid een steeds belangrijker onderwerp geworden op de agenda van overheden en publieke organisaties. De NIS-richtlijn eist van lidstaten dat zij naar behoren zijn uitgerust met een nationale cyberstrategie, een Computer Security Incident Response Team (CSIRT) en dat zij toezien op naleving van veiligheidseisen door aanbieders van essentiële diensten. De komende periode zal de toezichthoudende rol van de overheid steeds beter merkbaar worden bij commerciële bedrijven in de vitale sectoren. Gezamenlijk hebben zij de belangrijke opdracht om een werkwijze die daadwerkelijk onze nationale digitale veiligheid vergroot. Het is daarbij belangrijk dat de cultuur van risicobeheersing in deze samenwerking niet opeens omslaat in een compliance-gerichte aanpak. Het succes van de WBNI hangt in onze ogen af van succesvolle publiek-private samenwerking en de inzet van decentrale CERTS (bijvoorbeeld).

Samenwerking rondom incidenten

Tot nu toe worden significante cybersecurity-incidenten veelal intern door de geraakte organisatie afgehandeld. Met de invoering van de WBNI moeten organisaties in vitale sectoren ernstige incidenten melden bij het NCSC, waarna deze de impact van het incident kan analyseren en mogelijke mitigerende maatregelen in kaart brengen. Op basis van de informatie kan verdere impact van het incident op andere organisaties mogelijk worden voorkomen of beperkt. Dat versterkt niet alleen de nationale digitale veiligheid, maar ook de digitale veiligheid binnen de EU. Cyberaanvallen op organisaties kunnen een domino-effect hebben op andere sectoren en schade berokkenen over grenzen heen.

De verantwoordelijkheid om het incident te melden en het NCSC van de juiste informatie te voorzien ligt uiteindelijk bij de bedrijven die onderdeel uitmaken van de vitale sectoren. Echter, hoe vollediger, tijdiger en concreter de informatie is, hoe waardevoller voor de analyse en opvolging. Eerder is in Trends in Veiligheid al betoogd dat het delen van cyber-informatie een kwestie van vertrouwen is[1]. Informatie over cyberrsecurity-incidenten is vaak gevoelig, omdat het wat zegt over de (technische) security-maatregelen, de aard van data en systemen én de impact van het incident op de bedrijfsvoering. De natuurlijke neiging van private organisaties om bedrijfsgevoelige informatie zoveel mogelijk te beschermen staat daarmee op gespannen voet met het beoogde doel van de WBNI. Overheid en bedrijfsleven moeten daarom tijd en moeite investeren om, buiten de wettelijke vereisten om, te zorgen dat zij elkaar vertrouwen en leren begrijpen om belangrijke cyberinformatie met elkaar te delen.

Samenwerking met de toezichthouder

Een goede vertrouwensrelatie tussen de publieke en private sector is niet alleen essentieel zijn voor het melden van incidenten, maar ook voor het inrichten van een effectieve toezichthoudende rol van de overheid. Voor deze taak zijn een aantal toezichthoudende diensten aangewezen per sector (onder andere het Agentschap Telecom en De Nederlandsche Bank). Het is interessant om te volgen hoe deze toezichthoudende rol wordt ingevuld. Bemoedigend is dat bijvoorbeeld het Agentschap Telecom in 2019 al aangaf het stimuleren van de zorgplicht als een belangrijke taak te beschouwen[2]. Zoals eerder in dit artikel is betoogd, zou het de nationale digitale veiligheid sterk verstevigen als de bedrijven hun verplichting niet als 'compliance checklist' beschouwen, maar serieus werk maken van hun digitale veiligheid. De andere kant van de medaille is dat zij dan ook mogen verwachten van de toezichthouder dat deze oog heeft voor en ondersteuning biedt bij de risico-afwegingen. Daarom moet de autoriteit voldoende inspanning leveren om de soms complexe technische en bedrijfsmatige context mee te nemen in de oordeelsvorming. Nationale experts zullen de zakelijke-, en beveiligingsuitdagingen van bedrijven moeten begrijpen om een succesvolle audit uit te kunnen voeren.

De voorbeeldfunctie van de overheid

In de nieuwe situatie wordt het voor de overheid ook nog belangrijker om het goede voorbeeld te geven in de beveiliging van eigen diensten en infrastructuur om een geloofwaardige wetgever te zijn. Zowel de overheid als essentiële organisaties moeten zich realiseren dat het overtreden van de WBNI feitelijk betekent dat de nationale stabiliteit op het spel wordt gezet. Of dat dat in elk geval zo kan worden beschouwd in de maatschappij.

Samenvattend heeft de WBNI de potentie om een drijvende kracht te zijn om de security-volwassenheid van organisaties te versnellen en te borgen in de cultuur. Dit zorgt voor een nieuwe balans binnen bedrijven die er uiteindelijk toe moet leiden dat onze vitale infrastructuur beter wordt beveiligd.

In de weg daar naartoe, ontstaan nieuwe (invullingen aan) verantwoordelijkheden:

1. De rijksoverheid als toezichthouder op de digitale weerbaarheid en;
2. de vitale organisaties krijgen de wettelijke verantwoordelijkheid om de digitale veiligheid van hun diensten te borgen en incidenten te melden.

Om de WBNI succesvol te maken, ligt publiek-private samenwerking aan de basis. De volgende doelstellingen moeten gezamenlijk worden nagestreefd:

- De risico-management cultuur kan alleen duurzaam ontstaan als er een stevige governance structuur op het gebied van cybersecurity wordt ingericht.
- De organisaties moeten zorgen voor inzicht en transparantie rondom hun essentiële assets, zodat zij deze kunnen beschermen en snel en effectief kunnen reageren op incidenten.
- De overheid zal tijd en moeite moeten investeren om als toezichthouder een faciliterende rol te kunnen spelen.
- Informatiedeling rondom cyber-incidenten vereist een vertrouwensrelatie tussen overheid en private organisaties.

[1]Capgemini, Nederland digitaal veilig: internationale samenwerking als voorbeeld. https://www.trendsinveiligheid.nl/rapport/2018-vertrouwen-en-wantrouwen-in-de-digitale-samenleving/nederland-digitaal-veilig-internationale-samenwerking-als-voorbeeld/

[2]https://magazines.agentschaptelecom.nl/staatvandeether/2019/01/eidas-etd-wbni

Auteurs

Ana-Isabel Llacayo, CISM
Consultant Cybersecurity

ana.isabel.llacayo@capgemini.com

Ana-Isabel is gespecialiseerd in cyberveiligheid en EU-aangelegenheden. Ze werkt op het raakvlak van strategie en het technische domein. De afgelopen jaren heeft ze ruime ervaring opgedaan in het adviseren van publieke en private organisaties om zodoende hun cyberveiligheid te versterken.

Jasper van Buren
Managing Consultant Cybersecurity & Privacy

Jasper werkte ten tijde van het schrijven van het artikel bij Capgemini en hield zich bezig met adviesvraagstukken op het gebied van security-strategie, digitaal vertrouwen en de borging daarvan binnen organisaties en de samenleving.