Verslag bijeenkomst
''Digitale weerbaarheid: de bestuurder in control''

Introductie
Op woensdag 1 november vond de bijeenkomst 'Digitale weerbaarheid: de bestuurder in control'' plaats bij VNO-NCW. Op deze bijeenkomst ging moderator Kees Verhoeven in gesprek met de panelleden en de deelnemers in de zaal over het thema digitale weerbaarheid en de rol van de bestuurder en commissaris hierin. Eerst een korte introductie van deze bijeenkomst:
Digitalisering heeft de verhouding in de wereld veranderd, dit geeft ons kansen en tegelijkertijd ook uitdagingen. Een van deze uitdagingen zit toch wel in de digitale weerbaarheid.
Diginotar is een schitterend voorbeeld. We gaan het hebben over het voorkomen van incidenten. Een wisselwerking tussen overheid en bedrijven die dat aangaat.
De Europese Unie is er nu ook heel druk mee, denk aan: Dora, cyberresilience act (CRA), EUCS, NIS2 - dat kun je niet meer even overlaten aan de IT- afdeling. De bestuurders moeten hierin leidend zijn. Als bestuurder moet je op hoofdlijnen besluiten nemen en in control zijn.
Er is een technisch bestuurlijke kloof: aan de ene kant mensen die veel van techniek afweten, van auditing en certificeren en aan de andere kant de bestuurder. De bestuurder moet meer in control zijn. Het doel van vandaag is deze kloof te dichten en deze twee werelden dichterbij elkaar te brengen.

Wetgeving op het gebied van digitale weerbaarheid: wat komt er op de bestuurder af en hoe kunnen we hier gezamenlijk op voorbereiden? *Kees Verhoeven in gesprek met Angeline van Dijk (Inspecteur-Generaal bij de Rijksinspectie Digitale Infrastructuur en Martijn Lucassen (Adjunct-Directeur Digitale Economie bij het Ministerie van Economische Zaken & Klimaat)*
In het eerste deel wordt de strategische impact besproken: waar komt de wetgeving vandaan en wat komt er als bestuurder op mij af?

Verhoeven geeft het eerste panellid het woord; dit is Martijn Lucassen. De dreiging is de keerzijde van de digitale transitie. Criminele dreiging is er ook vanuit de hoek van staten (spionage). Criminelen kijken waar ze gemakkelijk kunnen binnenkomen. Daar moeten we ons tegen weren. Het vergroten van de cyberweerbaarheid is een gezamenlijke aanpak met andere lidstaten: criminelen kijken immers waar ze gemakkelijk kunnen binnenkomen. Een kwetsbare plek in een andere lidstaat kan gevolgen hebben voor de weerbaarheid in ons eigen land. Grondtoon van de strategie is dat er sprake is van een kanteling: burger, eindgebruiker en MKB: cybersecurity is je eigen verantwoordelijkheid. De complexiteit en aard van de dreigingen wordt groter en lastiger individueel te managen. Overheid probeert daar meer regie op te voeren, dit is straks niet meer vrijblijvend. Dit alles heeft consequenties voor alle stakeholders.
Er is veel nieuwe wetgeving. We proberen de regeldruk beheersbaar te houden. De strategie die neergelegd wordt door de overheid is om resilience en weerbaarheid te vergroten.
Cyberresilience act (CRA) introduceert een minimum veiligheidsstandaard voor digitale producten. Als het niet voldoet: aanspreken en handhaven. Deze act wordt nog over onderhandeld in Europa.
NIS2 zit meer op organisatieniveau. Alle bedrijven die essentieel zijn, hebben de zorgplicht dat hun netwerken en informatiebeheer veilig en op orde is. Hoe kun je die zorgplicht vormgeven.
Aanbieder van digitale producten en diensten worden op organisatieniveau aansprakelijk gesteld voor de veiligheid van hun producten en diensten.

Er is de uitnodiging om mee te denken in de voorbereiding op de NIS2 in de internetconsultatie in eerste kwartaal van 2024.

Nu is het aan Angeline van Dijk om het onderwerp te belichten vanuit het oog van de toezichthouder. Het is ook voor de toezichthouders heel ingewikkeld wat er nu allemaal op ons afkomt. Je hoeft als ondernemer niet bang te zijn voor de toezichthouder, we zoeken juist de verbindingen op. We willen samen op gaan in de ontwikkelingen. Er zijn al diverse publicaties geschreven:
- handreiking voor bestuurder van de Cybersecurity Raad
- handreiking bestuurstafel, geschreven voor de CISO en middenmanagement, om de bestuurder op weg te helpen van de RDI
- de evaluatietool gemaakt door RDI waarmee organisaties te weten kunnen komen of ze onder de NIS2-richtlijn vallen. De quickscan volgt nog om te zien hoe de ondernemer er voor staat.
Wat Angeline aan de deelnemers meegeeft: kom in gesprek en blijf in gesprek.

Voor digitale verantwoording zijn zaken in wording. Je moet het op orde krijgen als bestuurder. Dit vraagt om andere kennis, competenties en kwaliteiten: dit moet je opbouwen in je organisatie.
Ook het toezicht verandert. RDI wil aan de voorkant adviseren, over zorg- en meldplicht. Als de toezichthouder een boete moet geven, dan hebben eigenlijk beide partijen gefaald.
Martijn geeft aan dat de grondhouding wat incident gedreven is. Van reactief komen naar proactief. Incident gedreven naar structureel - wettelijke kaders - om vrijblijvendheid er af te halen.
Helpen/ondersteunen: bedrijven moeten in verbinding komen.
Financiële steun: Cyber Resilience Act: digitaal product op de markt, dan assessment door individueel bedrijf. Middelen ter beschikking zodat bedrijven daarbij worden geholpen.
Digital Trust Center is het loket om basisvragen over cyber hygiëne te beantwoorden.

Angeline geeft handelingsperspectief: Wacht niet op nieuwe wetgeving. wat kun je nu al doen? Aantal onderwerpen om mee aan de slag te gaan: Is het Business Continuïteit Management op orde? Welke processen zijn kritisch voor mijn functioneren? Maak een Impact Analyse, een crisisplan, zet een crisisorganisatie op en ga oefenen. Daar leer je van. Zorg voor inzicht in de supply chain: maak goede afspraken met leverancier als er wat gebeurt. Check en monitor de SSL met de leveranciers. Waar wil je wel/geen risico lopen. Ga het gesprek aan, waar kan je nog iets aan doen, maak een goede analyse en bedenk waar je bepaalde risico's accepteert.

De verslaggevingsstandaard: handvat voor bestuurders om bestuurlijke verantwoordelijkheid af te leggen voor IT-beheersing & Ervaringen vanuit CZ met deze standaard. *Door Irene Vettewinkel-Raymakers (Voorzitter NOREA) en Peter Slager (Chief Information Officer CZ)*
Kees geeft aan dat we een vertaling gaan maken van strategisch naar operationeel.
Irene Vettewinkel-Raymakers vertelt meer over het Norea reporting initiatief. Deze verslaggevingsstandaard is een handvat voor bestuurders om bestuurlijke verantwoordelijkheid af te leggen voor IT-beheersing. Geen controle framework, maar een werkwijze om tot een samenhangend verhaal te komen en als bestuur waar nodig te kunnen bijsturen.

Er is meer aandacht voor IT, digitalisering gaat in rap tempo vooruit. Zie dit ook als een stimulans om digitale weerbaarheid tussen de oren te krijgen. IT is de backbone voor een organisatie.
Digitale technologie biedt kansen maar ook dreigingen. Hoe gaan we als ondernemend Nederland om met al deze dreigingen. Het wordt steeds complexer omdat veel aan elkaar gekoppeld is. In het

woud aan certificeringen en rapportages is het moeilijk om door de bomen het bos te zien. ISO certificering als voorbeeld, NEN voor de zorgsector, SURF voor de onderwijssector als raamwerken en regels waar je aan moet voldoen en waarover je moet rapporteren. Accountant geeft verantwoording over het financiële deel. Is een klein onderdeel in het grotere geheel. Waar leg je verantwoordelijkheid over af: hoe fit is je onderneming?

Norea heeft het Norea Reporting Initiative ontwikkeld: een verslaggevingsstandaard over 6 onderwerpen. Verzameld door gesprekken met stakeholders en gegoten in een bepaalde structuur. Verslag wat terugkijkt maar ook vooruit kijkt. Met vragen zoals:
Hoeveel incidenten hebben we gehad, hoe snel is het opgelost? Outsourcing, hoe beheers ik dit? Wat zijn mijn toekomstplannen? Mogelijkheid om verantwoording af te leggen over de fitheid van je IT deel. Het is geen controleraamwerk. Het is belangrijk om een samenhangend verhaal op te schrijven samen met het bestuur. Voer de juiste dialoog en stuur bij waar nodig. Er is met veel stakeholders gesproken en er werden consultatierondes aangeboden, om te verbeteren. Daarnaast is Norea ook pilots aan het draaien met verschillende organisaties. Het idee is om dit verder uit te rollen.

Peter Slager vertelt over zijn ervaringen vanuit CZ met deze pilot van NOREA. Jurgen Pertijs is er ook bij omdat hij van de interne auditdienst is. CZ is maatschappelijke organisatie zonder winstoogmerk. Betaalbaarheid en toegankelijkheid binnen de zorg zijn uitdagingen. Strategie zit vol met digitaliseringsvraagstukken. We moeten veel meer vanuit de keten gaan denken.
CZ wil een datagedreven organisatie zijn. Intrinsiek gemotiveerd om alles bij elkaar te brengen.

Het doel bij de start van de pilot:

- Een integraal inzicht over het IT landschap heen
- Een gestructureerde wijze van het uitbrengen van een verslag
- Inzage op de IT beheersing, groei en ambities
- Inzage over de afgelopen 1,5 jaar en vooruit kijken naar de komende 1,5 jaar
- Overlap met het divisieplan, auditrapportages, self-assessments, Q rapportages, enz..
- Intern verslag en verklaring

CZ gaat dit binnenkort nog een keer doen, wat kunnen we hergebruiken? Volgende ronde ook meer business betrekken.

Pieter Jongstra: voorzitter Raad van Commissarissen van CZ is ook aanwezig bij deze bijeenkomst
De eerste reactie was sceptisch, niet weer een rapport, zien graag een geïntegreerd plaatje.
De belangrijkste rol is continuïteit van de organisatie, daar komt business en IT samen.
Hoe kun je de rol als raad van commissarissen goed vervullen. Permanente educatie is daarbij belangrijk geeft Pieter aan. Uiteindelijk is de pilot van meerwaarde geweest.

Een groep om aan te denken en mee te nemen is de ondernemingsraad. Heel veel aspecten vanuit security en strategie perspectief delen we met ondernemingsraad. Goede suggestie om dat te gaan doen.

Kees bespreekt een aantal stellingen met de deelnemers. De stellingen:
1. Als het gaat om digitale weerbaarheid ben ik (volledig) in control
2. De juiste en benodigde informatie bereikt mij tijdig
3. Ik wil dit thema de komende jaren hoger op de (bestuurs)agenda hebben

Reacties uit de zaal:
- Ik denk dat we niet in control zijn. Goed dat er wettelijke verplichting komt voor bestuurders om zich te verdiepen in digitale weerbaarheid. Als er geen stevige stok achter de deur staat, dan verandert er weinig.
- Ik heb geen overzicht meer over wat er allemaal aan zit te komen
- Ik vind het spannend wat er nog meer aankomt.
- Hoe kunnen we toewerken naar een manier om te voldoen aan de wet?
- Proof of the pudding is in the eating - je bent pas weerbaar als je bent aangevallen en dat hebt doorstaan.
- Wat kan de overheid doen? Het bestuur aansporen om zich voor te bereiden op NIS2. Het leeft nu nog onvoldoende.
- Aansprakelijkheid/verantwoordelijkheid: dat zijn nieuwe dingen.
- Veel mensen hebben gevoel dat ze veel moeten doen … Intrinsiek begrijpen en snappen waar risico's zitten, voor medewerkers, afnemers en consumenten.

Ter afsluiting van de bijeenkomst vond een geslaagde borrel plaats waarop de deelnemers verder spraken over het onderwerp digitale weerbaarheid.

Enquête
Achteraf is er een enquête verstuurd naar de deelnemers van deze bijeenkomst.
Het evaluatieformulier is niet door alle deelnemers ingevuld maar de respondenten gaven allen aan dat de bijeenkomst aan de verwachtingen voldeed.
Redenen om naar dit evenement te komen waren: informatie, contact met andere bestuurders, Bestuurlijke kant van cybersecurity, direct van belang voor mijn functie, verdere opbouw en "onderhoud" van mijn netwerk, horen van visie toezichthouders en netwerken met anderen betrokkenen.
Ook stelden we de vraag welke onderwerpen aan bod moeten komen bij toekomstige evenementen.
Antwoorden daarop waren:
- visie op AI
- meer praktische handreikingen (denk aan whitepapers)
- kennisontwikkeling op het gebied van compliance en risico-analyse
- uniformiteit in interpretatie en implementatie van wet- en regelgeving
- verdere wet- en regelgeving vanuit Europa
- on-premis vs hybrid cloud
- data residency
- meer over digitaliseringsbijlage bij accountantsverklaring