Position Paper:

Nationaal Cyber Security Lab Labsessie #1

"Op naar een zorgplichtstandaard voor cybersecurity"

Bernold Nieuwesteeg *(Directeur Centre for the Law and Economics of Cyber Security - Erasmus Universiteit Rotterdam)*
Petra Oldengarm *(Directeur Cyberveilig Nederland)*
Rutger Leukfeldt *(Directeur Centre of Expertise Cyber Security - Haagse Hogeschool)*
Michael Faure *(Hoogleraar Law and Economics - Erasmus Universiteit Rotterdam)*
Arnoud Engelfriet *(Algemeen directeur - ICTRecht)*
Hartger Ruijs *(Directeur en oprichter - Computest)*
René de Grauw *(Senior Consultant - Software Improvement Group)*
Nynke Brouwer *(Advocaat - Dirkzwager)*
Sjaak Schouteren *(Cyber Development Leader - Marsh)*

23 APRIL 2021

Introductie

Cyberincidenten, zoals datalekken en ransomware-aanvallen, zijn ook in het derde decennium van deze eeuw dagelijks in het nieuws. Het komt nog te vaak voor dat organisaties hun cybersecurity niet op orde hebben, een cyberincident te laat ontdekken en daar slecht op reageren. In de media krijgen getroffen organisaties, zoals recent de GGD[1], vaak de zwarte piet toebedeeld.

Het is echter niet terecht dat **alleen de afnemer** van software of hardware, zoals bijvoorbeeld de GGD, de wind van voren krijgt bij een cyberincident.

In de media en in beleidsdiscussies is onderbelicht dat een cyberincident vaak deels ook de 'schuld' is van de leverancier. Neem het voorbeeld van het datalek bij de GGD. De software (en daarmee ook de cybersecurity) van de GGD wordt niet door medewerkers van de GGD zelf ontwikkeld. Die zijn geschoold om vaccins toe te dienen en testen af te nemen. Voor wat betreft de gebruikte software zit hier vaak een softwareleverancier achter. Dat gegeven blijft buiten beeld als alleen de GGD negatief in de media uitgelicht wordt.

Cybersecurity is een verantwoordelijkheid van zowel afnemer als leverancier. Idealiter komen beide partijen vooraf tot goede afspraken over cyberrisico's, diensten en prijzen. En geeft de leverancier informatie en doet de afnemer zelf ook onderzoek. In het geval van de GGD bijvoorbeeld is het aannemelijk om te veronderstellen dat de softwareleverancier de potentie voor datalekken eerder kan voorzien en de GGD dus kan waarschuwen.

Die gedeelde verantwoordelijkheid is er in de praktijk vaak **niet**. Het Lab constateert onder andere:

1. Machtsongelijkheid in de markt zal blijvend leiden tot geduw om aansprakelijkheid bij de minst machtige partij te krijgen (dit is vaak de afnemer). De softwareleverancier sluit verantwoordelijkheid/aansprakelijkheid vaak uit in de leveringsvoorwaarden.
2. Marktwerking in het voordeel van de grote softwareleveranciers werkt. Er zijn geen grote Nederlandse softwareleveranciers waardoor de politiek en/of wetgeving hierop weinig invloed op kan uitoefenen.

Het Lab observeert dat idealiter:

1. Beide partijen vooraf tot goede afspraken komen over cyberrisico's, diensten en prijzen. De leverancier geeft informatie en de afnemer doet zelf ook onderzoek.
2. Er (model)voorwaarden van cyberverzekeringen zijn die betere beveiliging stimuleren, eventueel aan de hand van standaard risicoclassificatie.
3. Er objectieve criteria in de literatuur bekend zijn om risico's vast te stellen.

Er is dus een probleem dat dieper ligt dan alleen negatief uitlichten van organisaties die te maken hebben gehad met cyberincidenten en dan te verwachten dat zij het in de toekomst automatisch beter gaan doen. Namelijk een correcte verdeling van verantwoordelijkheid die zorgt dat er een optimaal samenspel komt tussen leverancier en afnemer. Een samenspel dat zorgt dat beide partijen optimale preventie, detectie en respons krijgen, gebruik makend van de kennis die bij beide partijen aanwezig is.

1. RTL (2021). https://www.rtlnieuws.nl/nieuws/nederland/artikel/5210644/handel-gegevens-nederlanders-ggd-systemen-data-base-coronit-hpzone

Veelal zal er vaker meer kennis over cybersecurity bij de leverancier liggen. In het voorbeeld van de GGD is het aannemelijk dat de softwareleverancier zich eerder bewust is van het cyberrisico dat ontstaat uit het breed toegang geven tot persoonsgegevens. Dan moet de softwareleverancier wel een prikkel hebben om die kennis te delen, hij moet een zorgplicht hebben (en aansprakelijk kunnen worden gesteld als de zorgplicht geschonden wordt).

Onze positie, een cybersecurity-zorgplichtstandaard

Cyberaanvallen (door onveilige hard- en software) kunnen resulteren in substantiële economische schade voor organisaties. Voor het borgen van de zorgplicht in B2B-relaties in de huidige aansprakelijkheidspraktijk, is het van belang om te kijken naar een oplossing die goed bestand is tegen de snel veranderende dynamiek in cybersecurity. Een regeling in Europese wetgeving is per definitie niet zinvol om de eenvoudige reden dat die snel verouderd zal zijn. Bovendien perkt dit de contractvrijheid te veel in.

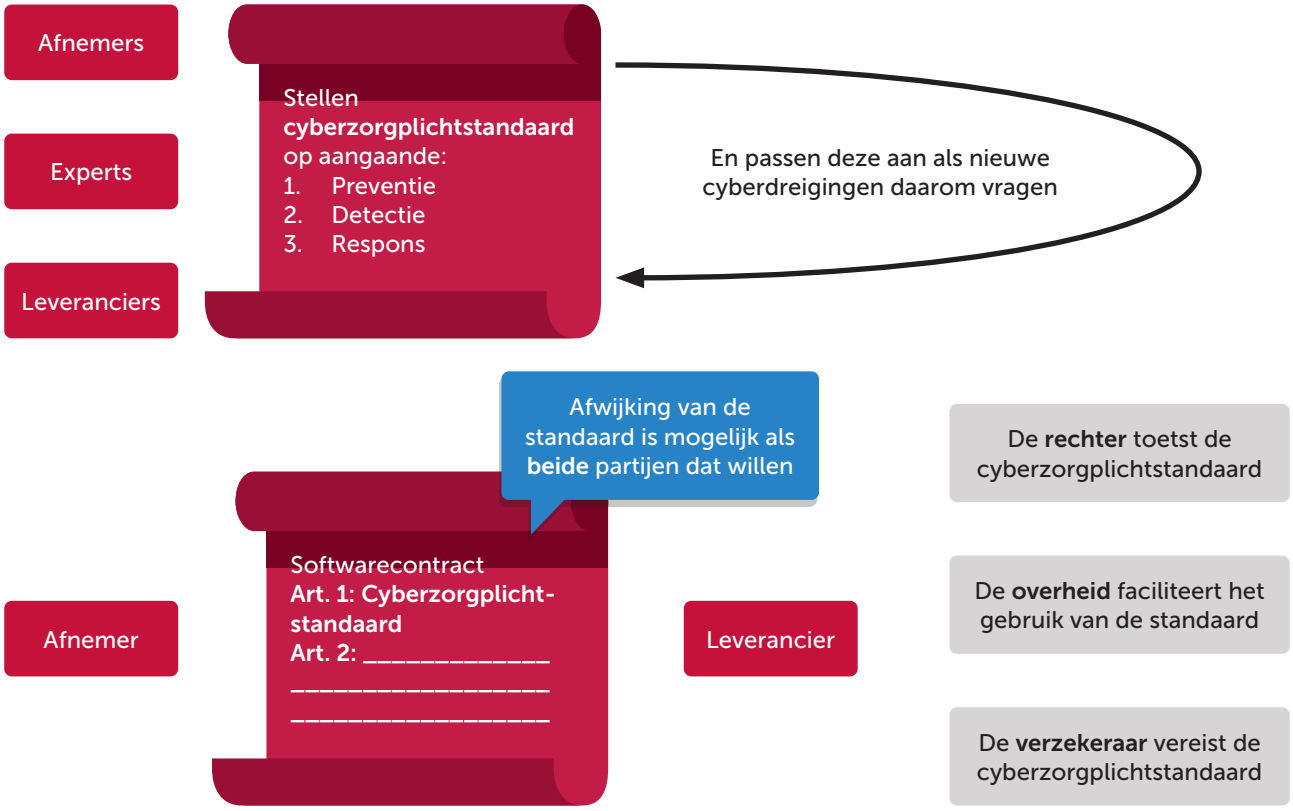
De oplossing is een cybersecurity-zorgplichtstandaard van hard- en softwareleveranciers die door middel van een set aan cybersecurityrichtlijnen in goed overleg door branches zelf via co-regulering opgesteld wordt.

Dit werkt op de volgende manier: branches (bijvoorbeeld de branche voor cybersecurityleveranciers, maar ook een branche die gebruikers vertegenwoordigt) en wetenschappelijke experts stellen cybersecurityrichtlijnen op die gelden als een standaard zorgplicht in een B2B contract. Deze richtlijnen bevatten regels over preventie, detectie en respons bij incidenten die gelden als een dienstverlener een product of dienst verkoopt.[2] Deze richtlijnen kunnen dan bijvoorbeeld in een contract tussen een administratiekantoor en een IT-dienstverlener aangaande de IT-beveiliging worden benut. Het is van groot belang dat de richtlijnen enerzijds door experts in partnerschap worden ontwikkeld en state-of-the art zijn, en dat ze tegelijk ook dynamisch zijn en de laatste nieuwe ontwikkelingen volgen. De richtlijnen moeten dus in dit brede overleg met branches en experts worden aangepast als de ontwikkelingen rondom cybersecurity daarom vragen. Als er bijvoorbeeld een nieuwe dreiging andere vormen van zorgplicht rondom detectie vraagt, zou dat toegevoegd moeten worden in de default zorgplicht.[3] Organisaties moeten in contracten aan de nieuwe dynamische cybersecurity-zorgplichtstandaard voldoen mits ze niet iets anders afspreken. Partijen zullen dat dan expliciet in het contract moeten opnemen.

2. Men kan ook denken aan subsets van regels voor verschillende type contracten, om fijnmaziger te werk te gaan.
3. Men kan ook op denken aan een jaarlijkse review van de zorgplichtstandaard waarin alle veranderingen rondom cybersecurity in tegelijk doorgevoerd worden.

Ons voorgestelde systeem is hieronder schematisch weergegeven:

Een flexibele & state-of-the-art cybersecurityzorgplichtstandaard



Aansluitend op dit (contractuele en zelfregulerings)systeem moet er een goed werkend verzekeringssysteem gestimuleerd worden voor zowel afnemer als leverancier. Voorwaarde daarvoor is wel dat er behoorlijk wat spelers op de cyberverzekeringsmarkt zijn die ook bereid zijn het product aan te bieden. Er moet dus een redelijk concurrerende verzekeringsmarkt zijn.Tevens is het ook van belang dat verzekeraars over diepgaande cybersecurity kennis beschikken om de verplichtingen van leveranciers te kunnen toetsen.[4]

Dat betekent in het ideale geval dat de verzekeraar ten aanzien van de verzekeringnemer (dit kan zowel de gebruiker zijn als leverancier die hij verzekert) bepaalde plichten oplegt met het oog op preventie, detectie en respons bij cybersecurity. Dit zal bijdragen aan het leveren van veilige digitale producten en diensten en het daadwerkelijk benutten van de zorgplichtstandaard richtlijnen voor de zorgplicht in de praktijk. Vervult de verzekeraar zijn rol goed, dan kan verzekering dus aan toenemende bewustwording bijdragen en een optimale preventie, detectie en response bevorderen.

4. In Nederland zijn er reeds verscheidene aanbieders op de cyberverzekeringsmarkt aanwezig die in toenemende mate kennis ontwikkelen en bijdragen aan bewustwording. Het verder stimuleren van deze verzekeringsmarkt biedt dus kansen om het systeem van de zorgplichtstandaard goed te laten werken.

Call to Action

1. Wij roepen het komende kabinet op om werk te maken van de cyberzorgplichtstandaard door afnemers, experts en leveranciers bij elkaar te brengen.
2. Wij roepen het komende kabinet op om zich in Europees verband hard te maken voor het opstellen van Europees-brede standaardisatie (zonder dat dit in een keurslijf van een bindende richtlijn wordt gegoten).
3. Wij roepen de rijksoverheid op om het goede voorbeeld te stellen met een aantal inkoopvoorwaarden/eisen over security geclassificeerd naar klein/groot/middel risico/ omvang, zodat de markt deze kan volgen.
4. Wij roepen op tot een verdere ontwikkeling van feitenrechtspraak waarin een duidelijkere lijn kan worden ontdekt in software-aansprakelijkheid.

Over het Nationaal Cyber Security Lab (NCSL)

Nederland heeft behoefte aan maatschappelijke oplossingen voor optimale cybersecurity buiten de bestaande kaders. Door wetenschappers en bedrijfsleven bijeen te brengen combineert het NCSL wetenschappelijke inzichten met best practices vanuit het bedrijfsleven. De overheid is klankbord. Het Lab bestaat uit een bureau dat labsessies organiseert. Het bureau selecteert thema's en genodigden per labsessie. Tijdens de labsessie faciliteert het bureau het creatieve proces. Na de labsessie wordt een position paper met een kernachtige weergave van de oplossingen openbaar gemaakt en verspreid.