



Onderwerp: verzoek om deelname aan onderzoek over kosten en baten van cybersecurity

Wat is de aanleiding?

Om het verdien- en concurrentievermogen van de economie van Zuid-Holland te beschermen en te vergroten heeft de Economic Board Zuid-Holland eind 2020 een Cybersecurity Roadmap vastgesteld. Het doel is om de komende jaren gericht en structureel de digitale veiligheid en weerbaarheid van de regionale topsectoren te verhogen. Dat gebeurt met concrete acties en onderzoeksactiviteiten om te zorgen voor maatwerk en de juiste oplossingen per sector.

Wat is er aan de hand?

Steeds vaker lees je in de media over bedrijven die het slachtoffer worden van verschillende vormen van cybercrime. Gevolgen van deze vorm van criminaliteit kunnen financieel zijn, maar ook is er vaak sprake van reputatie en fysieke schade. Cybersecurity bedrijven trekken aan de bel met alarmerende boodschappen dat veel bedrijven hun cybersecurity niet op orde hebben en veel meer moeten investeren. Hierbij gooien ze alle bedrijven en organisatie op een grote hoop. Niet gek dat zij deze algemene boodschap uitdragen vanuit commerciële overwegingen. Deze boodschap doet alleen geen recht aan de grote diversiteit aan bedrijven, risico's, mensen, en sectoren. Hoe weet jij wat voor jouw maakbedrijf of organisatie de juiste cybersecurity investeringen zijn? Hoe weet jij welke risico's je loopt? Hoe maak je een goede risico-kosten-baten afweging?

Wat willen we doen?

De TU Delft en de Erasmus Universiteit Rotterdam hebben (als LDE-consortium) een subsidie gekregen van de Gemeente Den Haag om te onderzoeken hoe individuele bedrijven en organisaties afwegingen maken op het gebied van cybersecurity. Om beter onderscheid te kunnen maken tussen al die verschillen, en daarmee beter inzicht te geven in wat er écht op het spel staat. Dat moet bedrijven helpen om beter te kunnen bepalen welke cybersecurity investeringen voor hen slechts 'nice to have' en welke echt 'need to have' zijn. Om dat goed te onderzoeken moeten de onderzoekers klein beginnen met één groep in een bepaalde sector en wij denken dat de Slimme Maakindustrie hiervoor een interessante doelgroep is.

Wat hebben we nodig en wat levert het voor jullie op?

We vragen organisaties maximaal 45 minuten van hun tijd vrij te maken om inzicht te geven in de wijze waarop ze tot beslissingen komen op het gebied van cybersecurity. Dit doen we door middel van een survey en een beknopt interview. We vragen organisaties dus niet om actuele kwetsbaarheden te delen, maar om, op een voornamelijk abstract niveau, te reflecteren op de wijze waarop zij omgaan met cybersecurity. Vragen die aan bod komen zijn onder andere:

- Welke (data)bronnen gebruiken organisaties nu om een investeringsbeslissing in cybersecurity te doen en hun cybersecuritystrategie te bepalen?
- Welke (data)bronnen zouden gewenst zijn om een (nog) betere afweging te kunnen maken?
- Welke verhalen/aneddotes zijn van belang geweest in het bepalen van het cybersecuritybeleid?
- Wat voor incidenten zijn er in het verleden geweest en hoe is daarmee omgegaan?



Universiteit
Leiden

 **TU**Delft

Erasmus
University
Rotterdam



Dit combineren wij met andere vormen van data verzamelen, onder andere het raadplegen van publieke bronnen en dreigingsinformatie. Hiermee beogen we inzichten te verkrijgen in jullie sector, die we uiteindelijk ook graag weer met jullie delen. Potentiele inzichten kunnen zijn:

- Een overzicht van de databronnen die organisaties nu gebruiken (directe relevantie deelnemende organisaties)
- Een potentieel aan ongebruikte databronnen (dit zou direct relevant kunnen zijn voor de deelnemende bedrijven)
- 'Best practices' ten aanzien van het gebruik van anekdotes en (data)bronnen (ook directe relevantie voor de deelnemende bedrijven)
- Bredere (academische) inzichten gerelateerd aan het structureel verbeteren van de kosten van cybercrime en cybersecurity op sectorniveau.

To put it simple: door mee te doen (een tijdsinvestering van maximaal een uur) kan je betere investeringsbeslissingen aangaande cybersecurity maken waardoor je beter beveiligd bent tegen cyberaanvallen. Ook draag je ermee bij aan een cyberveiliger maaksector.

Bereid om mee te helpen?

Neem dan zo spoedig mogelijk contact op met Rens Hoogerwaard: hoogerwaard@law.eur.nl

We hopen de interviews de komende maanden af te nemen.