Hoe uw organisationele cyberveiligheid opkrikken?

16 maart 2022, 01:00

Annanda Rath

De actuele omstandigheden maken meer dan ooit duidelijk dat zich als bedrijf beschermen tegen cyberaanvallen allerlei geen overbodige luxe is. Maar hoe kunt u uw organisationele cyberveiligheid verbeteren? We helpen u alvast op weg: afspraak in Brussel of Antwerpen!

We merkten dat niet alleen de toename van ransomware-aanvallen, maar nu ook de precaire geopolitieke situatie rond Oekraïne en de daarmee gepaard gaande cyberdreiging heeft geleid tot vragen van grote ondernemingen. Zij maken zich zorgen over de cyberrisico's die ze lopen via hun toeleveringsketen.

De grotere ondernemingen liggen wakker van de volgende twee vragen:

1. Hoe veilig zijn onze gegevens bij onze leveranciers?
2. Hoe cyber-resilient zijn onze leveranciers? Zullen ze bij de eerste de beste cyberaanval hun diensten of producten aan ons nog kunnen leveren?

Het is duidelijk dat digitaal vertrouwen en digitale veerkracht geen 'nice to have' onderwerpen meer zijn, maar absoluut noodzakelijk voor bedrijven die groeiambities hebben. Uw prospecten en klanten willen ervan overtuigd worden dat uw bedrijf een veilige keuze is om mee samen te werken.

Met dit gegeven in het achterhoofd organiseren we tweemaal een masterclass over het opkrikken van uw organisationele cyberveiligheid. Het goede nieuws is dat er nog plaatsen vrij zijn voor de masterclass in Brussel (vrijdag 22 april) en in Antwerpen (woensdag 1 juni).

Op het programma

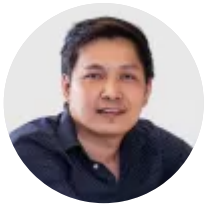
- Algemene kadering van cybersecurity binnen IT en Risk Management
- Hoe garandeer je digitale veiligheid?
- Frameworks en certificatie, bv. CIS Controls, ISO 27001
- De 5 functies van cybersecurity
- Hoe begin je aan het opstellen van een risk-based cybersecurity-strategie?
- Oefening: risk assessment, business impact analyse, threat modelling
- Typische threat actoren, trends
- Kadering oorlog Oekraïne en Russische cyberdreiging
- Hoe verlopen de meeste aanvallen typisch?
- Veiligheidscultuur, en hoe steun krijgen van het topmanagement?
- Leren van 'veiligheid' in andere sectoren
- 30 praktische, pragmatische stappen die je kan toevoegen aan je cybersecurity roadmap

- Hoe omgaan met cybersecurity vragenlijsten (assessments) die je krijgt van nieuwe of bestaande klanten?
- Hoe gaan jullie om met het risico dat jullie zélf lopen via jullie eigen toeleveranciers? Welke vragen stel je best?
- Discussie over cyberverzekeringen
- Hoe kan je een beroep doen op financiële hulp van VLAIO?
- Samenvatting, en next steps voor jullie

Er wordt veel nadruk gelegd op discussies tussen de deelnemers, praktische toepasbaarheid en pragmatisme. Voor bedrijven die ooit ambiëren om ISO 27001 gecertifieerd te worden, vormt deze opleiding de basis foundation.



Auteurs



Annanda Rath