Interview met Paul Slootmaker, CISO KPN

Assetmanagement is de basis van alles, dat moet op orde zijn

6 december 2021

Wilfried Olthof en Thomas Wijsman

(Publicatiedatum: 6 december 2021)

Via Teams spreken we met Paul Slootmaker, RE en bovendien CISO van KPN, sinds oktober 2019 de opvolger van Jaya Baloo. Haar interviewden we ruim vijf jaar geleden. Onwillekeurig terugdenkend aan dat interview concluderen we dat welbespraaktheid en aanstekelijk enthousiasme blijkbaar tot de vaste functie-eisen voor KPN CISO's behoren. Ook Paul zit vol ideeën, die in een klein uur naar buiten vloeien.

Paul, kun je ons vertellen hoe je hier terecht bent gekomen?

'Ik werk al zo'n twaalf jaar bij KPN in het werkveld van cybersecurity en riskmanagement. Mijn start hier maakte ik als IT-riskmanager in de tweede lijn. Daar deed ik bij verschillende onderdelen opdrachten op het terrein van IT-risk en IT-compliance. Mijn achtergrond ligt in IT en IT-audit. In 1999 begon ik als systeemprogrammeur bij Capgemini, om vervolgens over te stappen naar de IT-auditpraktijk van Arthur Andersen. Via een tussenstap bij KPMG kwam ik na de ondergang van Andersen in dienst van KPN. Ik was weliswaar primair IT-auditor, maar ben ook altijd nadrukkelijk geïnteresseerd geweest in de implementatiekant en consultancy. Het auditvak is een uitstekende leerschool geweest, die ik hiernaartoe meebracht.'

Hoe zie je de organisatie van de afdeling voor je?

'Ik heb jullie interview van vijf jaar geleden met mijn voorgangster nog even nagelezen. Zij gaf jullie onder meer aan hoe ze bezig was de CISO-functie en de organisatie van de afdeling vorm te geven. Dat was iets waar we toen samen aan hebben gewerkt. Ze schetste een structuur met een Corporate Emergency Respons Team, het CERT, een *Red Team* met *ethical hackers* en een *Security Operations Centre*, het SOC, in de rol van *Blue Team*. Jaya heeft beslist iets moois tot stand gebracht en daar bouw ik op voort. En ik heb veel van haar geleerd.'

‘Maar laat ik eerst wat meer context geven. Als IT-riskmanager in de tweede lijn was ik verantwoordelijk voor de decentrale Risk & Compliance-afdeling van het voormalige Getronics, dat in 2011 door KPN was overgenomen. In 2014 besloot KPN deze decentrale afdeling te centraliseren. Als IT-riskmanager had ik regelmatig contact met Jaya en er ontstond een uitstekende werkrelatie tussen ons. Op een gegeven moment vroeg ze: “Paul, waarom kom je niet bij mijn afdeling werken? Ik heb op dit moment nog niet echt een specifieke functie voor je, maar wil je me helpen de Security-afdeling verder op te bouwen?” Ze stelde één voorwaarde: ik moest mijn Risk & Compliance-bagage bij de voordeur achterlaten. “Daar doen we hier niet aan, hier doen we security”, sprak ze kordaat. En security, dat zag ze als overwegend rule-based. Nu ik het stokje van haar heb overgenomen, ben ik met het team bezig de volgende stap te maken. Rule-based beleid is een prima basis. Maar business-overwegingen en een klemmender wordend dreigingsbeeld door externe ontwikkelingen maakten het nodig om daarnaast toch ook een meer risk-based aanpak te ontwikkelen. We werken dan ook intensief samen met de collega’s uit de tweede en derde lijn (Risk en Audit).’

> *“Dreigingsbeeld wordt klemmender door externe ontwikkelingen*

Dat betekent dus activiteiten erbij?

‘Ja, we hebben we bijvoorbeeld nieuwe activiteiten ontwikkeld vanuit de *security lifecycle* gedachte. De eerste stap is het maken en uitdragen van beleid: *prevent*. Gevolgd door een sterke *detect and response capability* inrichten. Wat we daarna hebben toegevoegd is meer en beter inzicht geven in hoe succesvol we zijn in het veilig houden van de KPN-omgeving. Dit doen we onder meer met het doel de monitoring en rapportage naar onze stakeholders inzichtelijk te maken. Dat betreft de verificatie van geïmplementeerde maatregelen, en ook compliance. Compliance en security liggen in elkaars verlengde. Ik zie het zo: compliance is de basis, de vloer, en security het plafond. Als IT-auditor kan ik m’n specifieke expertise inzetten om beide werelden met elkaar te verbinden.’

Binnen NOREA denken we na hoe organisaties zich op basis van een 'IT-auditverslag' kunnen gaan verantwoorden over hun grip op IT. Hoe kijk jij daar tegenaan?

'Je moet de stakeholder-behoeftes geïntegreerd afdekken. We hebben te maken met ISAE 3402-trajecten, waarbij we op basis van assurancerapporten verantwoording afleggen aan externe partijen in de zakelijke markt. We zijn met ons accountantskantoor EY in gesprek hoe we de 3402-rapportages over cybersecurity en informatiebeveiliging kunnen stroomlijnen. We richten nu ook een framework in waarmee we meten wat de effectiviteit van de KPN Security Policy is. Die policy is een baseline met zo'n duizend maatregelen. Die moet je natuurlijk niet allemaal willen toetsen, dat is onbegonnen werk, dus ben ik op zoek naar de *key-controls*.'

'Van bijzonder belang voor ons is momenteel de recente ministeriële Regeling veiligheid en integriteit telecommunicatie, een regeling onder de Telecomwet. De regeling schrijft voor dat we aantoonbaar moeten voldoen aan negentien beheersmaatregelen voor de telecomsector. De overheid heeft deze maatregelen opgelegd met het doel de Nederlandse

van statelijke actoren. Hierover moeten we ons verantwoorden naar het Agentschap Telecom. Het afgelopen jaar hebben we al concrete ervaring met het thema "statelijke dreigingen" opgedaan. Het ging om netwerkapparatuur van leveranciers die volgens de nationale autoriteiten mogelijk onder controle staan van geopolitieke tegenstrevers. Deze geopolitieke context wint snel aan belang en heeft dus ook impact op ons werk als security-afdeling.'

Hoe kijk je aan tegen de geopolitieke knelpunten die zichtbaar beginnen te worden?

'Daar zijn we natuurlijk alert op. Je ziet inderdaad verschuivingen in het geopolitieke spectrum. De traditionele machtsverhoudingen beginnen minder vanzelfsprekend te worden. We houden als telecomoperator het geopolitieke spectrum dan ook goed in de gaten en nemen daar onze maatregelen op. Binnen die context is het mijn taak een veilig netwerk te bieden. We kijken daarbij niet naar bepaalde grootmachten, en ook is ons beveiligingsbeleid leveranciersonafhankelijk.'

> *"In control-verklaringen en frameworks moet je verbinden met de technische wereld van de Red Teamers*

Leidt de roep om externe verantwoording niet tot minder aandacht voor interne verantwoording?

'Zeker niet. Belangrijker dan de verantwoording naar de toezichthouder vind ik de verantwoording binnen de organisatie zelf. Zonder een serieuze, openhartige interne verantwoording over de eigen operatie is verbetering een illusie. De interne hygiëne moet bijvoorbeeld aantoonbaar op orde zijn en daarover geven we dan ook assurance. De basis van security ligt in het managen van assets, patches, vulnerabilities en configuraties, en in het adequaat acteren op verbeterpunten en incidenten. Daarover legt de tweede lijn intern verantwoording af. Ik vind dat we als security-afdeling de onderneming en de bedrijfsonderdelen en operaties tot die verantwoording moeten bewegen. Daarbij is het balanceren tussen hulp en dwang. Onder meer bieden we steun door ze een instrumentarium voor de verslaglegging in handen te geven.'

Hoe zie je de relatie tussen in control-verklaringen en frameworks aan de ene kant en de technische wereld van de Red Teamers aan de andere kant?

'Je moet die twee met elkaar verbinden en het beste van de twee werelden verenigen. Neem bijvoorbeeld een van de tollgate-regels, die onze organisatie verplicht alle innovaties te onderwerpen aan pentests. We hebben per jaar misschien wel 200 to 250 nieuwe producten en andere innovaties. Daarbij hebben we steeds vaker te maken met internationale providers van cloud services zoals SAAS, IAAS en PAAS. Dat zijn sterke partijen die niet op voorhand accepteren dat KPN hun beveiliging wil testen en in plaats daarvan met een algemene SOC2- of SOC3-verklaring of met een eigen pentestrapport zwaaien. Onze pentesters vertrouwen die dan weer niet omdat die niet is toegesneden op de specifieke situatie bij KPN. Ik zoek naar een aanpak waarin we kunnen steunen op de verschillende typen verklaringen van een externe partij, waarbij ook voor pentestrapporten een kwaliteitsmaatstaf ontstaat, zoals we die voor auditrapportages gewend zijn te hanteren. Dan nog houd ik als auditor altijd goed rekening met de beperkingen van een dergelijke verklaring en welke verantwoordelijkheden en maatregelen je aan de gebruikerskant moet nemen.'

Klinkt lang niet eenvoudig

'Nee, elke keer weer merk ik hoe complex KPN als bedrijf eigenlijk is. Je hebt de netwerk-kant, met de technische infrastructuur waar de telecomnetwerken onder vallen en je hebt de IT-kant, waarin de hele IT is georganiseerd rondom die netwerken om ze in de lucht te houden, ze te bewaken en om uiteindelijk de netwerkdiensten te kunnen leveren. Daarnaast hebben we nog een IT-kant voor de verkoop van IT-diensten aan de zakelijke markt. En tenslotte hebben we veel bedrijven overgenomen en geïntegreerd – of half geïntegreerd dan wel doorverkocht. Alles bij elkaar hebben we dus een supercomplex geheel van netwerken. Dan is kennis van IT, riskmanagement en security absoluut noodzakelijk maar op zichzelf niet toereikend. Je hebt daar bovenop vooral ook inzicht in de totale samenhang nodig: *understanding the business* is dan ook de werkelijke basis voor onze activiteiten.'

> *Assetmanagement is de basis van alles*

Wat zijn je grootste uitdagingen? Zijn dat de cyberdreigingen of de zorg dat je afdeling goed geëquipeerd is, met budgetten en de juiste expertise?

'Dat vind ik een lastige keuze – ze strijden om voorrang. De cyberdreigingen zijn vanuit de geopolitieke context bijzonder relevant. Daartegen bestand blijven is de rode draad door het werk dat ik doe, maar dat is abstract geformuleerd. De feitelijke dreigingen zijn maar al te reëel, ook voor een prima beveiligd bedrijf als KPN. Denk bijvoorbeeld aan de ransomware-aanvallen die nu in criminele kringen bijzonder populair zijn. Of het via malware heimelijk server-capaciteit van anderen gebruiken voor cryptomining. Assetmanagement is de basis van alles, dat moet in orde zijn. Maar ook aan de menskant en op het vlak van alle andere resources moet de fundering solide zijn. Ook dan nog resteren er genoeg uitdagingen waarvoor we ons met ons volle gewicht in de strijd moeten werpen. Ons werk heeft impact en doet ertoe. Permanent, je kunt geen moment tevreden achterover leunen om successen te vieren.'

Tot slot: zie je ook kansen als tegenhanger van de uitdagingen en constante dreigingsdruk waar jullie mee geconfronteerd worden?

'Jazeker. Recent ben ik bijvoorbeeld uitgenodigd voorzitter te worden van de Commissie Vitale Infrastructuur, terwijl KPN CEO Joost Farwerck is herbenoemd in de Cybersecurity Raad, met de portefeuille Vitale Sectoren. Voor de goede orde: niet namens KPN, we zijn benoemd als onafhankelijke deskundigen die in die gremia handelen zonder last of ruggenspraak. Deze contacten geven mooie kansen om ook persoonlijk stappen vooruit te kunnen zetten.'

Drs. Th. (Thomas) Wijsman RE | coach en strategisch adviseur

Gepokt en gemazeld bij de Algemene Rekenkamer is Thomas Wijsman nu actief als coach en strategisch adviseur. Hij is opgeleid in IT, IT-audit, psychologie en coaching, en combineert zo hard en soft skills. Daarnaast is hij actief in verschillende commissies van Norea.

Drs. W. (Wilfried) J.A. Olthof | directeur bij *NOREA*

Wilfried Olthof is directeur van NOREA en heeft daarvoor functies vervuld bij de Perscombinatie, het ministerie van VROM en de Vrije Universiteit Amsterdam. Hij heeft Politicologie en Bestuurswetenschappen gestudeerd.