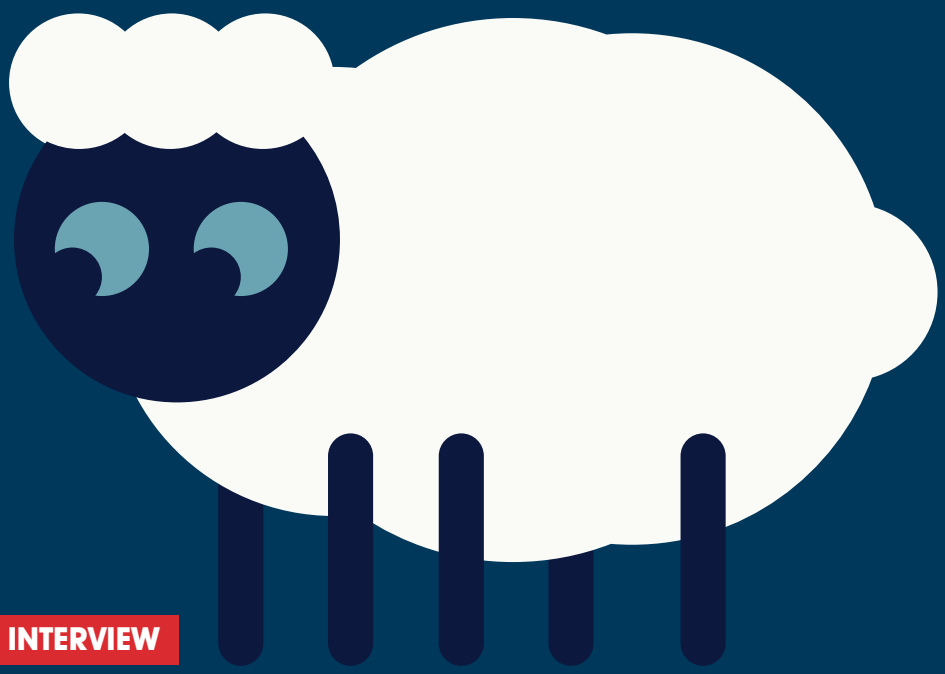
Auteurs: Nicole van Deursen is redactielid van iB-Magazine. Nicole van Deursen is bereikbaar via nicolevandeursen@pvib.nl. Sandra Kagie is freelance tekstschrijver (Sanscript tekstproducties). Sandra is bereikbaar via info@sanscriptproducties.nl.



INTERVIEW

Tekort aan securityspecialisten

‘Stop met zoeken naar het schaap met de vijf poten’

Cybersecurity specialisten zijn en blijven lastig te vinden. Dat bedrijven en organisaties vacatures op dit vlak moeilijk ingevuld krijgen, heeft echter niet alleen te maken met een tekort aan talenten. Zelf kunnen en móeten bedrijven volgens Mark Ruijsendaal van het nationale veiligheids-cluster Security Delta (HSD) meer doen om mensen te interesseren voor het vakgebied en misschien nog wel belangrijker om de juiste mensen te behouden voor het vak van informatiebeveiliging. “Wanneer ik nu naar de sector als geheel kijk, zie ik vooral een onvolwassen onderwijs- en arbeidsmarkt. Een opgave voor ons allemaal om dit te veranderen”, roept hij op.

Met de term 'onvolwassenheid' doelt programmamanager Ruijsendaal bijvoorbeeld op 'het allegaartje aan eisen' dat hij tegenkomt in vacatureteksten van bedrijven en organisaties die op zoek zijn naar een cybersecurity specialist. "Ik zie irreële eisen en vacaturenamen die alle kanten op vliegen. Dat maakt het vakgebied onaantrekkelijk omdat geïnteresseerden op basis van dit allegaartje geen idee hebben over hun loopbaanpad en ontwikkelmogelijkheden", geeft hij aan.

Realistische vragen en eisen

Structuur en uniformiteit aanbrengen in vacatureteksten door gemeenschappelijk taalgebruik te hanteren, ziet hij dan ook als een belangrijke opgave voor de sector. "Maak hiervoor gebruik van de profielen die er zijn. Zo leg je gezamenlijk een heldere basis voor een ontwikkeling naar volwassenheid van de sector", luidt zijn hartenkreet. Waarbij hij bijvoorbeeld verwijst naar de functieprofielen en competenties zoals deze zijn opgesteld door het PvIB. Ook roept hij ons als beroepsvereniging op organisaties te helpen realistische vragen en eisen te stellen aan een potentiële kandidaat. "Nu zoekt iedereen het schaap met de vijf poten, zo niet acht poten. Een kandidaat moet dertien talen beheersen, drie systemen kennen, sinds zijn dertiende jaar bezig zijn met computers hacken en als persoon over een waslijst aan certificeringen beschikken. Kijk naar wat je vraagt en vraag je af of de eisen realistisch zijn om te vragen van één persoon."

Human Capital Agenda Security

Binnen Security Delta, waarbinnen zo'n 275 bedrijven, overheidsorganisaties en kennisinstellingen samenwerken om het verschil te maken in de veiligheid van onze digitaliserende samenleving, houdt Ruijsendaal zich als senior programmamanager onder meer bezig met de Human Capital Agenda Security (1). Een programma gericht op het aantrekken en ontwikkelen van talent en het oplossen van de mismatch tussen vraag en aanbod als het gaat om (cyber)security talent. En een programma dat Security Delta heeft opgesteld samen met een veertigtal partners voor een periode van vier jaar, 2019-2022.

Dat er na 2022 een nieuwe agenda komt, staat al vast. Het tekort aan security specialisten blijft immers een urgent vraagstuk. Hoe groot het tekort in Nederland echter is, vindt Ruijsendaal lastig aan te geven. Ook dit heeft volgens hem te maken met de 'onvolwassenheid van de sector'. "Het tekort wordt niet goed gemeten en in kaart gebracht", legt hij uit.

De vraag welke functies er nu precies vallen onder de noemer cybersecurity specialist, vindt hij bijvoorbeeld al lastig te beantwoorden. "Systeem- en applicatiebeheerders of een integraal risico manager, zijn dat cybersecurity specialisten?", vraagt hij zich af. Sowieso is het geen beroep dat door het Centraal Bureau voor de Statistiek standaard in kaart wordt gebracht. Reden voor Security Delta om met de Provincie Zuid-Holland een landelijke arbeidsmarktmonitor te maken en om vacatures te analyseren (2).

De talentpool vergroten

Eén van de doelen van Ruijsendaal en zijn collega's voor dit jaar is ervoor te zorgen dat er een nieuwe studie verschijnt met betrekking tot het aanbod en de mismatch op de cybersecurity arbeidsmarkt, zo kondigt hij aan. Een studie die als basis zal gaan dienen voor de nieuwe Human Capital Agenda Security 2023-2026. Daarbij noemt hij voor dit jaar de ontwikkeling van een programma om zij-instromers te interesseren voor het cybersecurity domein als een belangrijke doelstelling (zie cybersecuritywerkt.nl). De huidige aanwas voorziet namelijk niet in de bestaande en verwachte toekomstige vraag naar talent. Door de toenemende awareness voor cybersecurity in zijn algemeenheid zal de vraag naar professionals alleen maar verder toenemen, zo is zijn verwachting.

"Kijkend naar het MKB, denk ik dat de beer nog niet ontwaakt is", geeft Ruijsendaal aan. "Het grote volume in de vraag naar security talent moet in dit segment nog komen. Het gaat hier niet om staatsgeheime informatie die beschermd moet worden, maar toch kunnen succesvolle hacks ook hier grote (economische) impact hebben. Wanneer het ons samen niet lukt om aan de alsmaar toenemende vraag naar security talent te voldoen, zal onze veiligheid verder onder druk komen staan. Daarvan ben ik overtuigd."

Talent behouden

Behalve voor de noodzaak om te werken aan de instroom van nieuw talent, vraagt Ruijsendaal daarom ook nadrukkelijk aandacht voor het behoud van talent binnen het vakgebied. "Ik zie in de praktijk een uitstroom van security professionals in de tweede en derde fase van hun carrière", waarschuwt hij. Ook hier noemt hij het gebrek aan een helder carrière- en ontwikkelperspectief als een van de oorzaken. "Mensen zien geen ontwikkelmogelijkheden meer of voelen zich onvoldoende gewaardeerd en na een aantal jaren van bijvoorbeeld 24/7 ploegendiensten incident management of bij onderbezetting wreekt zich dat in uitval en uitstroom."

“Het grote volume in de vraag naar security talent binnen het MKB moet nog komen: de beer is nog niet ontwaakt.”

Automatisering van cybersecurity, denk aan de toepassing van Artificial Intelligence, ziet hij hier slechts als een deel van de oplossing. “Dit biedt kansen om het werk interessanter te maken”, legt hij uit. “Maar het risico van overbelasting blijft. Er blijft immers op basis van AI zoveel (analyse)werk te doen.”

“Cybersecurity heeft drie kanten: techniek, organisatie en mensen”, gaat hij verder. “Specialisten vanaf hbo-niveau worden vaak geacht op al deze vlakken te acteren. Met als gevolg dat ze ten prooi vallen aan roofbouw.”

‘Denk in teams’

Wat Ruijsendaal betreft moeten organisaties dan ook veel meer in cyberteams gaan denken waarin verschillende functies geclusterd zijn. Teams waarin een cybersecurityprofessional samenwerkt met bijvoorbeeld een risicoanalist, een applicatie-ontwikkelaar, een netwerkbeheerder, een beleidsmaker en een HR-adviseur. Zo creëer je breed draagvlak binnen je organisatie voor security door het onderwerp integraal te benaderen en onderdeel van je bedrijfscultuur te maken. Door de workload te verdelen wordt het werk bovendien behapbaar en daarmee duurzaam aantrekkelijker.

Een tip die Ruijsendaal organisaties vervolgens geeft, is om voor de samenstelling van dit soort integrale teams nadrukkelijk intern te kijken. “Vaak zijn er al medewerkers in alle geledingen die in cybersecurity geïnteresseerd zijn en over de nodigde competenties beschikken. Wanneer je dit verborgen talent vindt, hoef je extern niet meer op zoek en daarbij bied je deze medewerkers nieuw perspectief. Het mes snijdt zo aan twee kanten.”
Blijkt het opzetten van een cyberteam voor een (kleinere) organisatie een brug te ver dan is uitbesteden van je IT-security een optie. “Ook dit vraagt echter de nodige kennis en kunde vanuit het management, inkoop en HR”, stelt hij. “Zij moeten zorgen voor de juiste balans tussen zelf doen en uitbesteden. Waarbij wat Ruijsendaal betreft ontwikkeling van eigen talent, vanuit het oogpunt van draagvlak binnen een organisatie, de voorkeur heeft.

Rol overheid?

Tot slot vragen we de programmamanager van Security Delta of hij in de oplossing van het vraagstuk van het tekort aan securityspecialisten een rol ziet voor de overheid. Die ziet hij zonder meer, maar niet exclusief. Als grootste werkgever vindt hij dat de overheid in de eerste plaats ervaringen moet delen met de private sector. “Hoe zorgt de overheid voor integraal beleid door in alles wat ze doen aandacht te vragen voor cybersecurity, hoe houden zij talent vast en hoe zorgen zij voor ontwikkelperspectief voor hun mensen?”, somt hij op. “Ervaringen waar de private sector van kan leren.”

Vervolgens komt hij op het punt van opleidingen. Cybersecurity zou wat hem betreft veel meer verankerd moeten zijn in allerlei opleidingen. Niet alleen in IT-opleidingen, maar juist veel breder. Hij noemt het voorbeeld van het ROC Mondriaan in Den Haag dat met specifieke modules niet alleen binnen IT-opleidingen, maar juist ook binnen niet-technische studies, denk aan zorgopleidingen, aandacht besteed aan het onderwerp. Modules die ook beschikbaar zijn voor andere ROC’s. Dit alles om breder competenties te ontwikkelen. Iets waar wat Ruijsendaal betreft vanuit de overheid, ook op hbo- en wo-niveau, meer op gestuurd zou moeten worden in het kader van het maatschappelijk belang van opleidingen. Iets dat hij nu mist. “Onderwijs, bedrijfsleven en organisaties zoals HSD en PvIB moeten het samen met de overheid doen.”

Referenties

(1) https://securitydelta.nl/media/com_hsd/report/231/document/HSD-Human-Capital-Agenda-Security-Webversie.pdf
(2) Securitytalent.nl https://securitytalent.nl/career/dashboard