International Cyber Security Summer School loont de moeite

Interview: Douwe Mik, EY

Cybersecurity-specialisten liggen niet voor het oprapen. Toch weet EY in één dag vijf nieuwe experts aan zich te binden. "We zijn hard op zoek naar nieuwe mensen", vertelt Douwe Mik, partner cybersecurity bij EY. "In Nederland groeit onze cybersecurity-tak met zestig procent per jaar." Terugblikkend constateert hij tevreden dat het een goede zet was om als medeorganisator te investeren in de International Cyber Security Summer School.

In zes dagen tijd krijgen zestig studenten en promovendi diepgaande kennis over cybersecurity aangereikt. Zij volgen lezingen en werken aan uitdagende opdrachten van vooraanstaande internationale en binnenlandse organisaties. Dit is in het kort de opzet van de International Cyber Security Summer School (ICSSS). EY is een van de organisatoren van de vierde editie, in augustus 2018. Ook HSD, NATO, Europol, Universiteit Leiden en Dutch Innovation Factory behoren tot de organisatoren. In het kader van access to talent worden geïnteresseerde studenten en organisaties bij elkaar gebracht tijdens een kennisintensief lesprogramma over de ins en outs van cybersecurity.

Onderbelicht

EY vult een van de zes dagen in. In de ochtend is er een plenair programma met lezingen, onder andere van oud-premier Jan-Peter Balkenende, partner bij EY. Hij schets de bredere context van cybersecurity op het gebied van nationale en internationale veiligheid, wetgeving en politiek. Daarna gaan de studenten in twee groepen uiteen. De ene groep richt zich op de techniek. Onder leiding van ethische hackers krijgen zij te maken met security operations, incident respons en slaan ze als team aan het hacken. De andere groep volgt gedeeltelijk het zelfde programma en gaat concreet aan de slag met risk management en cybersecurity-beleid. Douwe Mik: "Aan het eind van de dag brachten we de groepen weer bij elkaar, met als boodschap: cybersecurity draait om mens, techniek en proces. Alle drie mogen niet onderbelicht blijven in een organisatie die cybersecure wil zijn."

Cyberscholing hard nodig

De investering in de vierde editie van de International Cyber Security Summer School loont de moeite: vijf studenten treden in dienst bij EY. Ook heeft EY inmiddels ook enkele alumni van eerdere edities in dienst. De ICSSS is volgens Mik een goed voorbeeld van de kracht van het veiligheidscluster HSD en van de samenwerking met HSD Office. Mik: "Samenwerken betekent dat je ook zelf actief moet zijn. De kwaliteit van de output heeft alles te maken met input die je er zelf in stopt. Als partner van HSD kan je niet achterover leunen in de verwachting dat de gebraden kippetjes wel worden doorgeschoven. Als je bereid bent te investeren in wat HSD te bieden heeft, dan pluk je daar de vruchten van." Met die gedachte draagt EY ook zijn steentje bij aan de Cyber Security Week en aan netwerkbijeenkomsten. Maar dat is niet de enige reden. "Als EY delen we onze kennis en voorzien we in trainingen vanwege het maatschappelijk belang dat we zien. Dat doen we binnen HSD, maar ook bij hogescholen en universiteiten. Cyberscholing is namelijk hard nodig, want we zien te weinig talent in de markt. Dit zou in onderwijsland veel meer prioriteit moeten krijgen."

Slim investeren

Human capital is voor de snelgroeiende cybersecurity-tak van EY een begrijpelijk speerpunt. Op verschillende gebieden zijn experts nodig, waarbij het weerbaar maken van klanten de rode draad is door alles heen. "Cybersecurity kent veel facetten, maar op hoofdlijnen richten wij ons op mens, techniek en proces", vertelt Mik. "Je kan alles wel dichttimmeren, maar de mens blijft een cruciale

factor. We laten zien waar de kwetsbaarheden en ingangen tot het bedrijfsnetwerk zich bevinden. Als het gaat om techniek, maken we inzichtelijk wat het huidige beschermingsniveau is en waar dat verbeterd kan worden. Het is daarbij te kort door de bocht om te zeggen dat er meer geïnvesteerd moet worden. Vaak is dat niet zo. Er moet slimmer geïnvesteerd worden." Mik doelt hierbij op het derde onderdeel: proces. Op basis van het dreigingslandschap vindt een risicoanalyse plaats, waarna daarop aansluitend de governance en het risicobeleid wordt ingeregeld. "Iedereen is een target, maar het risicoprofiel verschilt per organisatie. Door dit goed in beeld te brengen zijn we in staat onze klanten zelfstandig weerbaar te maken tegen cyberaanvallen."