De studenten van vandaag, zijn onze collega's van morgen. Tijd om hen in het zonnetje te zetten! In deze nieuwe rubriek willen we de stagiairs informatiebeveiliging aan het woord laten. We leren een stagiair kennen aan de hand van diens vooropleiding, zijn of haar verhaal over hoe iemand in de informatiebeveiliging terecht is gekomen, bij welke organisatie de stage gelopen wordt en wat de stage-opdracht is. **Meld ook jouw stagiair aan bij de redactie!**

Stage lopen als onderdeel van je studie

Mijn naam is Luiza Atas. Ik ben een vierdejaars student Integrale Veiligheidskunde op de Avans Hogeschool in Breda. Ik heb gekozen voor deze studie omdat ik graag wat wil bijdragen aan de veiligheid van onze maatschappij. Voor mijn derdejaars stage heb ik onderzoek uitgevoerd voor het Expertisecentrum Security (ECS), een onderdeel van de gemeente Den Haag.

De opleiding Integrale Veiligheidskunde heeft mij bewust gemaakt van hoe breed en hoe belangrijk veiligheid is. Tijdens de studie werd mij geleerd om veiligheidsvraagstukken vanuit juridische, economische, psychologische en de bestuurskundige kant te bekijken. Ook heb ik geleerd om problemen te signaleren, projecten op te zetten en de veiligheid te bewaken bij grootschalige rampen. Dit binnen de overheid, bedrijven, binnen de zorg of in woonwijken. Verder heb ik verschillende vaardigheden kunnen ontwikkelen zoals presenteren, interviewen, discussiëren, onderzoeken, communiceren, adviseren, managen, leidinggeven en analyseren. De opleiding Integrale Veiligheidskunde duurt vier jaar. De kennisvakken die worden aangeboden vind je in de tabel hiernaast.

Er wordt individueel of in groepen gewerkt aan praktijkopdrachten. De opdrachten komen zowel uit het publieke- als het private domein. Je leert risico's in kaart brengen en afwegen. Hierbij worden problemen vanuit verschillende

Leerjaar 1	Recht, Veiligheid en Middelen, Veiligheid en Trends, Criminologie en Integrale Veiligheid
Leerjaar 2	Arbeidsveiligheid, Veiligheid en Trends, Securitymanagement, Veiligheid en Informatie, Engels en Veiligheid en Middelen
Leerjaar 3	Stage
Leerjaar 4	Minor en Afstudeerstage

invalshoeken bekeken.

Keuze voor een stage

De opleiding Integrale Veiligheid is heel breed, waardoor ik het lastig vond om een stage uit te zoeken. De opleiding focust zich op de fysieke veiligheid terwijl onze docenten ons bewust maken dat digitale veiligheid net zo belangrijk is. Dit trok mijn aandacht en hoewel ik een passie heb voor criminologie en psychologie, wilde ik me ook meer verdiepen in digitale veiligheid. Als maatschappij beginnen we ons immers steeds meer bewust te worden van het feit dat cybercriminaliteit toeneemt. Jammer genoeg is het voor veel mensen nog een raadsel hoe zij zich daadwerkelijk kunnen beschermen tegen dit fenomeen dat zich nog dagelijks ontwikkelt. Het leek mij leuk om te leren hoe we onze persoonlijke gegevens en gevoelige informatie digitaal kunnen beschermen. Het Expertisecentrum Security, een afdeling die zich bezighoudt met de informatieveiligheid van één van de grootste gemeentes van Nederland, leek mij de ideale plek om hierover meer te leren.

De gemeente Den Haag is een openbare instantie. Hiermee wordt een overheidsorganisatie aangeduid die rechtspersoonlijkheid bezit. De gemeente wordt bestuurd door bestuursorganen. Dat zijn de raad, het college van burgemeester en wethouders en de commissies. De gemeente Den Haag is opgedeeld in zeven diensten: Bestuursdienst (BSD), Dienst Bedrijfsvoering (DBV), Dienst Publiekszaken (DPZ), Dienst Stadsbeheer (DSB), Dienst Onderwijs, Cultuur en Welzijn (OCW), Dienst Sociale Zaken en Werkgelegenheidsprojecten (SZW) en Dienst Stedelijke Ontwikkeling (DSO). Tijdens mijn stage heb ik meegekeken met de dienst Bedrijfsvoering, afdeling Informatisering en Automatisering waarbij het ECS hoort. Het Expertisecentrum bestaat uit vijf subgroepen. De taken die zij uitvoeren zijn de kaders en beleidstukken voor de informatieveiligheid van de gemeente opstellen en het uitdragen en adviseren over de implementatie ervan. Het beleidskader is uitgewerkt met specifieke interne documenten voor informatieveiligheid op tactisch niveau en werkinstructies op operationeel niveau.

Invulling stage

Tijdens mijn stage heb ik meegelopen met de werkgroep binnen het ECS die zich bezighoudt met het faciliteren van het proces rond de Baseline Informatiebeveiliging Overheid (BIO)-zelfevaluatie. Dit is een intern proces waar gemeentebreed aan functioneel beheerders wordt gevraagd om aan te geven of en hoe de verplichte BIO-maatregelen binnen hun applicatie tot stand zijn gekomen. Een procesverantwoordelijke neemt eigenaarschap over de antwoorden van de functioneel beheerder en vervolgens wordt de zelfevaluatie teruggekoppeld aan het Expertisecentrum Security. Zij adviseren de proceseigenaren daarna bij het verbeteren van beveiligingsmaatregelen. Om de implementatie van de BIO-maatregelen te vergemakkelijken heeft het ECS vergelijkbare maatregelen geclusterd en deze smartcontrols genoemd. Het zelfevaluatie proces is continu in ontwikkeling. Ik wilde graag een steentje bijdragen aan het verbeteren hiervan. Tijdens mijn stage heb ik twee hulpmiddelen ontwikkeld: De BIO-Verbeterrapportage en de BIO-Spiekbriefjes. De BIO-Verbeterrapportage wordt gebruikt door functioneel beheerders en procesverantwoordelijken. Het doel ervan is het bewustzijn vergoten, overzicht te bieden en werkzaamheden te vergemakkelijken. De rapportage is specifiek bedacht voor Multi Disciplinaire Teams (MDT) waarbinnen ambtenaren met verschillende functies samenwerken om een concreet vraagstuk op te lossen. Er is hiervoor gekozen om het bewustzijn van informatiebeveiliging te verhogen en onderlinge samenwerking te stimuleren. De rapportage zou ook per applicatie gebruikt kunnen worden.

De BIO-Verbeterrapportage bestaat uit: een inleiding, aanleiding, doelstelling, prioritering, verwachting en resultaat waarmee duidelijk wordt gemaakt waar de BIO-Verbeterrapportage voor is. Vervolgens is een inhoudsopgave toegevoegd om gemakkelijk bij specifieke informatie te komen. Na de inhoudsopgave komt het deel waarin per BIO-hoofdstuk de basis gelegd wordt voor verbetering van BIO-maatregelen. Hierin wordt de smartcontrol benoemd, de bijbehorende uitleg (duiding) en het risico van het niet-implementeren van de BIO-maatregel/smartcontrol. Het risico is toegevoegd om het belang van (verbetering van) implementatie van een BIO-maatregel/smartcontrol aan te geven. Na de risico's wordt per applicatie(s) een overzicht gegeven van de door de functioneel beheerder ingevulde verklaring in de zelfevaluatie. Tot slot geven de adviseurs informatieveiligheid van het expertisecentrum security een review op de ingevulde verklaring in de zelfevaluatie en een beschrijving met concreet advies.

Het tweede hulpmiddel dat ik heb ontwikkeld is/zijn de BIO-Spiekbriefjes. Het doel van de spiekbriefjes is het bewustzijn te vergoten en werkzaamheden te vergemakkelijken. De spiekbriefjes zijn gebaseerd op de BIO. De BIO is geschreven in een taal die over het algemeen moeilijk te begrijpen is voor mensen die niet uit het vakgebied komen. Om het begrijpen van de BIO wat eenvoudiger te maken heb ik spiekbriefjes gemaakt op basis van de Cyberspiekbriefjes (1). Voor elk BIO-hoofdstuk is een Spiekbriefje gemaakt. Hierin kun je lezen waar het hoofdstuk over gaat, wat het belang ervan is voor de gemeente Den Haag, wat de gevolgen zijn bij misbruik en waar je eventueel meer informatie kunt vinden over het hoofdstuk.

Conclusie

Ik heb een hele uitdagende stage gehad waarin ik nieuwe mensen heb ontmoet, veel heb geleerd en mezelf heb kunnen ontwikkelen op individueel en professionele vlak. Verder ben ik bewust geworden van wat informatieveiligheid daadwerkelijk is en hoe informatiebeveiliging wordt gemanaged in praktijk. Tijdens mijn stage ben ik enthousiast geworden om deze kennis met iedereen te delen.

Mochten er vragen zijn dan ben ik te bereiken via luizaatas@outlook.com.

Referenties:

(1) zie Cyberspiekbriefjes (veiliginternetten.nl)