Hanzehogeschool Groningen
University of Applied Sciences

Vak: Beveiliging en Organisatie — credits: 4

Vakcode	ITVB18SCY2
Naam	Beveiliging en Organisatie
Studiejaar	2019-2020
ECTS credits	4
Taal	Nederlands
Coördinator	H.T. Keulen
Werkvormen	Hoorcollege Opdracht
Toetsen	Practicumopdracht - Overige toetsing Tentamen B&O - Computer, organisatie tentamenbureau

Leeruitkomsten

De student:
- geeft aan wat de termen "risico", "bedreiging", "kans van optreden (mate van dreiging)" en "impact (maximale schade)" betekenen en onderbouwt dit
- weet welke rollen er in een organisatie vaak te maken hebben met verschillende onderdelen van informatiebeveiliging en kan het verschil herkennen tussen eindverantwoordelijkheid en uitvoeringsverantwoordelijkheid (eigenaarschap)
- voert een risicoanalyse uit koppelt de uitkomsten aan een set van beveiligingsmaatregelen
- weet welke normen voor informatiebeveiliging er zijn, past deze toe, en concretiseerd de maatregelen uit een norm
- weet wat het verschil tussen strategische, tactische en operationele documenten is en kan dit duiden
- stelt een concreet advies op en onderbouwt dit
- weet hoe een informatiebeveiligingsproces ingericht kan worden (voor welke activiteiten heeft een security officer een verantwoordelijkheid) en hoe je dat borgt in de PDCA cyclus (opstellen beleid, vaststellen beleid, implementeren beleid, communiceren over beleid, evalueren beleid, actualiseren beleid)
- weet wat de onderdelen van een BCP zijn en kan dit duiden en toepassen
- geeft aan aangeven welke controles er mogelijk zijn, wat het verschil is, en kan dit duiden
- weet wat de termen "MAPGOOD", "beschikbaarheid", "integriteit", en "vertrouwelijkheid" betekenen, en kan deze duiden
- past gezond boeren verstand toe

Inhoud

In dit onderdeel ga je specifiek inzoomen op de tooling en methoden om de organisatie te adviseren omtrent informatiebeveiliging. Als leidraad nemen we onderdelen van het internationale CISSP opleidingstraject. Een belangrijk onderdeel hierbij is de risico analyse met daarbij het opstellen van tegenmaatregelen die passend zijn. De focus ligt daarbij op de organisatorische aspecten van beveiliging, zoals beleid, fysieke beveiliging, disaster recovery planning, en business conntinuity.

Opgenomen in opleiding(en)

HBO-ICT, Major Network & Security Engineering

School(s)

Instituut voor Communicatie, Media & IT