beroepsonderwijs bedrijfsleven

Keuzedeel mbo

Security in systemen en netwerken 2

gekoppeld aan één of
meerdere kwalificaties mbo

Code

K0444

Penvoerder: Sectorkamer ICT en creatieve industrie
Gevalideerd door: Sectorkamer ICT en creatieve industrie
Op: 10-11-2015

1. Algemene informatie

D1: Security in systemen en netwerken 2
Studielast
240
Beroepsvereisten
Nee
Certificaten
Ja

Scholingsbehoefte/landelijke herkenbaarheid
De wereld wordt steeds 'digitaler' en het thema cybersecurity wordt daarmee steeds belangrijker. De keuzedelen Security in systemen en netwerken 1 en 2 richten zich op een aantal specialistische informatiebeveiligingstaken die verder gaan dan de beveiligingstaken die een reguliere ICT beheerder uitvoert. Naast signaleren en implementeren van beveiligingsmaatregelen zijn ook de sociaal-communicatieve vaardigheden en een integer en ethische gedrag een belangrijk onderdeel van de keuzedelen. Het beter inspelen op specifieke cybersecurity-onderwerpen is een actuele vraag vanuit de arbeidsmarkt, het behalen van dit keuzedeel is dan ook voor werkzoekenden en werkenden van grote meerwaarde.

Ingangsdatum certificaat
01-10-2016

Gekoppeld aan kwalificatie(s)
Zie bijlage op www.s-bb.nl/kwalificatiedossiers
Toelichting

Dit keuzedeel Security in systemen en netwerken 2 is een vervolg op keuzedeel Security in systemen en netwerken 1. Het is aan te bevelen eerst het keuzedeel Security in systemen en netwerken 1 te volgen.

De keuzedelen sluiten aan op de door het Platform voor Informatiebeveiliging ontwikkelde opleidingsprofiel voor de ICT Security Specialist 1 (ICTSS1). De keuzedelen Security in systemen en netwerken 1 en 2 werken tezamen toe naar een in ontwikkeling zijnde standaard voor de arbeidsmarkt.

Relevantie van het keuzedeel
De wereld wordt echter steeds 'digitaler' daarmee wordt cybersecurity steeds belangrijker. Om op de arbeidsmarkt in te kunnen spelen op specifieke cybersecurity-onderwerpen of om beter voorbereid naar (specifieke) opleidingen in het hbo door te stromen is het behalen van het betreffende keuzedeel een pré.
Het keuzedeel Security in systemen en netwerken 1 geeft een voor de arbeidsmarkt en doorstroom relevante uitbreiding op aan het kwalificatiedossier.

Beschrijving van het keuzedeel
Het keuzedeel Security in systemen en netwerken 2 gaat in op het volgen van technologische ontwikkelingen om een beeld te krijgen van de actuele dreigingen en beveiligingsmogelijkheden. Het vergelijken van gegevens uit de monitoring en testen van de werking van de beveiligingsmaatregelen met het beveiligingsplan. Het doen van voorstellen van beveiligingsaanpassingen en het implementeren van beveiligingsaanpassingen. Daarnaast zijn de sociaal-communicatieve vaardigheden en een integer en ethische gedrag een belangrijk onderdeel van het keuzedeel.

Branchevereisten

Aard van keuzedeel
Verdiepend
Doorstroom

2. Uitwerking

D1-K1: Implementeert beveilingsaanpassingen

Complexiteit

De beginnend beroepsbeoefenaar werkt in een groot bedrijf in een gestructureerde en voorspelbare omgeving en in een klein bedrijf in een gestructureerde omgeving die soms ook onvoorspelbaar kan zijn. Hij voert zijn werkzaamheden uit aan de hand van richtlijnen, protocollen en procedures. Deze werkzaamheden zijn hiermee gestructureerd van aard. Het vinden van oplossingen op de diverse beveiligingsvraagstukken zorgen voor grote diversiteit in deze werkzaamheden. Om de veiligheidsvraagstukken op te lossen heeft de beginnend beroepsbeoefenaar specialistisch kennis en vaardigheid nodig. De voor de beroepsbeoefenaar benodigde kennis dient continu onderhouden te worden: het vakgebied is snel en blijvend in ontwikkeling.
De complexiteit van het werk wordt vergroot door de benodigde houding en competenties om een cyberaanval te voorkomen.

Verantwoordelijkheid en zelfstandigheid

De beroepsbeoefenaar werkt samen met gelijken en leidinggevenden/ specialisten (ook wel security officer genoemd). Hij draagt verantwoordelijkheid voor resultaten van eigen activiteiten. De complexere werkzaamheden voert de beginnend beroepsbeoefenaar uit onder begeleiding en dan ligt de eindverantwoordelijkheid bij de leidinggevende/ specialist.

Vakkennis en vaardigheden

De beginnend beroepsbeoefenaar:

- heeft specialistische kennis van de belangrijkste technieken voor informatiebeveiliging en hun toepassingen.
- heeft specialistische kennis van de belangrijkste beperkingen en kwetsbaarheden van gangbare en opkomende informatietechnologie
- heeft specialistische kennis van oplossingen t.b.v. beveiliging in informatiesystemen en netwerk, incl. cloud en mobiele apparatuur

- kan resultaten van monitoring en testen interpreteren
- kan risico-analyse en informatiebeveiligingsplan lezen
- kan oplossingen t.b.v. beveiliging zoals in de cloud en mobiele apparatuur implementeren
- kan herstelactiviteiten formuleren na een ernstig ICT-incident
- kan voorstellen voor beveiligingsaanpassingen presenteren en uitleggen aan leidinggevende/ specialisten

D1-K1-W1: Volgt technologische ontwikkelingen op het gebied van ICT-beveiliging

Omschrijving

De beginnend beroepsbeoefenaar volgt de belangrijkste technologische ontwikkelingen op het gebied van ICT-beveiliging in diverse bronnen. Hiermee schat hij bedreigingen in voor de veiligheid van netwerken en systemen en vormt zich een beeld van de actuele ontwikkelingen op het gebied van ICT-beveiliging.

Resultaat

Een actueel beeld van bedreigingen en beveiligingsmogelijkheden

Gedrag

De beginnend beroepsbeoefenaar
- verzamelt actief en uitgebreid relevante informatie uit verschillende bronnen.
- blijft alert op mogelijk nieuwe informatietechnologieën op het gebied van ICT-beveiliging en bestudeert mogelijk nieuwe toepassingen.

De onderliggende competenties zijn: Onderzoeken

D1-K1-W2: Doet voorstellen voor beveiligingsaanpassingen

Omschrijving

D1-K1-W2: Doet voorstellen voor beveiligingsaanpassingen

De beginnend beroepsbeoefenaar vergelijkt de gegevens uit de monitoring en testen van de werking van de beveiligingsmaatregelen met het beveiligingsplan en de verzamelde informatie over opkomende bedreigingen en beveiligingsmogelijkheden. Hij formuleert voorstellen voor beveiligingsaanpassingen conform het beveiligingsplan in een rapport. Hij presenteert de voorstellen aan de leidinggevenden/ specialist.

Resultaat

Rapport met voorstellen voor beveiligingsaanpassingen is besproken met leidinggevende/ specialist

Gedrag

De beginnend beroepsbeoefenaar
- evalueert de gegevens grondig en met vaktechnisch inzicht, maakt op basis van de beschikbare feiten logische gevolgtrekkingen en rationele inschattingen en weegt voor- en nadelen tegen elkaar af om tot een voorstellen van beveiligingsaanpassingen te komen.
- presenteert zichzelf helder en deskundig bij de bespreking van de voorstellen voor beveiligingsaanpassingen met de leidinggevende/ specialist.
- handelt naar eer en geweten in overeenstemming met de geldende normen, waarden en regels.
- rapporteert helder en volledig de resultaten van de monitoring en testen van de werking van de beveiligingsmaatregelen.
De onderliggende competenties zijn: Vakdeskundigheid toepassen, Ethisch en integer handelen, Formuleren en rapporteren, Presenteren, Instructies en procedures opvolgen

D1-K1-W3: Voert beveilingsaanpassingen uit

Omschrijving

De beginnend beroepsbeoefenaar inventariseert de uit te voeren activiteiten voor het doen van beveiligingsaanpassingen. Hij plant en organiseert deze in tijd, benodigde middelen en mensen. Hij voert de beveiligingsaanpassingen uit.

Resultaat

Beveiligingsaanpassing zijn conform het informatiebeveiligingsplan uitgevoerd.

Gedrag

De beginnend beroepsbeoefenaar
- toont vaktechnisch inzicht bij het formuleren van herstelactiviteiten en het uitvoeren van en het implementeren van beveiligingsaanpassingen.
- betrekt, waar nodig, tijdig de juiste collega's bij het uitvoeren van beveiligingsaanpassingen en stemt de activiteiten vervolgens met hen af.
- houdt rekening met de impact van aanpassing op de infrastructuur
- houdt zich bij het uitvoeren van beveiligingsaanpassingen aan de werk- en veiligheidsprocedures en handelt als een rolmodel.
- blijft onder druk en spanning (bijv. bij ernstige ICT-incidenten) objectief in het beoordelen van en handelen naar omstandigheden.

De onderliggende competenties zijn: Vakdeskundigheid toepassen, Plannen en organiseren, Instructies en procedures opvolgen, Met druk en tegenslag omgaan