beroepsonderwijs bedrijfsleven

Keuzedeel mbo

Basis cybercriminaliteit en cyberveiligheid

Code

K1352

Ontwikkeld door: Aventus; Saxion; Politie; More2safety
Penvoerder: Sectorkamer zakelijke dienstverlening en veiligheid

1. Algemene informatie

D1: Basis cybercriminaliteit en cyberveiligheid
Studielast
240
Beroepsvereisten
Nee
Certificaten
Ja Onderwijsinstellingen kunnen, onder specifieke voorwaarden, in de derde leerweg een certificaatgerichte opleiding aanbieden voor een keuzedeel dat na 1 augustus 2020 is vastgesteld. Zie vragen 7 en 17 van de veelgestelde vragen veranderaanpak (https://kwalificatiestructuur-mijn.s-bb.nl/vragen/verander). **Scholingsbehoefte/landelijke herkenbaarheid** Als gevolg van de verschuiving van traditionele criminaliteit naar online criminaliteit (bron: CBS, 2022) hebben werkgevers in de beveiligingsbranche en ordehandhaving te maken met een tekort aan medewerkers met kennis op het gebied van digitale veiligheid en cybercriminaliteit. Dit resulteert in een scholingsbehoefte op het gebied van digitale handhaving, beveiliging en opsporing. Deze scholingsbehoefte wordt onderschreven door verschillende partijen in de beveiligingsbranche en ordehandhaving, waaronder de Politie Oost-Nederland. Door het certificaat Basis cybercriminaliteit en cyberveiligheid in te zetten voor de (bij)scholing van werkenden kan aan deze scholingsbehoefte worden voldaan en de digitale veiligheid worden verbeterd. **Zelfstandige betekenis** Na het volgen van dit scholingstraject zijn werkenden beter en breder inzetbaar in de beveiligingsbranche en ordehandhaving. Ze kunnen cyberdreigingen en cybercriminaliteit herkennen en een rapportage opstellen waarin o.a. maatregelen worden voorgesteld. **Doelgroep** Dit certificaat is bedoeld als basis voor werkenden bij de politie en organisaties in de beveiligingsbranche en ordehandhaving die in hun eerder gevolgde opleiding en/of opgedane werkervaring geen specifieke vaardigheden hebben opgedaan op het gebied van digitale beveiliging. **Ingangsdatum certificaat** 27-04-2024
Ontwikkeld voor kwalificatie(s)
Zie bijlage op www.s-bb.nl/kwalificatiedossiers
Toelichting
Relevantie van het keuzedeel Het werkveld beveiliging en handhaving krijgt meer en meer te maken met cybercriminaliteit en vanuit de beroepspraktijk komt steeds meer vraag naar mensen met kennis van ict in relatie tot criminaliteit, handhaving/beveiliging en politie. **Beschrijving van het keuzedeel** Centraal in dit keuzedeel staan kennis, vaardigheden en competenties op het gebied van cybercriminaliteit en cyberveiligheid. De deelnemer verkrijgt basiskennis van verschillende vormen van cybercriminaliteit, van methoden die cybercriminelen toepassen en van beveiligingsmethoden. De deelnemer is met deze basiskennis in staat om mogelijke risico's te signaleren van een persoon, website of kleine organisatie en daarvan een rapportage op te stellen. **Branchevereisten** Nee **Aard van keuzedeel**

D1: Basis cybercriminaliteit en cyberveiligheid
Verbredend

2. Uitwerking

D1-K1: Cyberdreigingen signaleren en beveiligingsmaatregelen voorstellen

Complexiteit

De beginnend beroepsbeoefenaar voert de werkzaamheden veelal volgens een vast patroon uit. De werkzaamheden zijn gestructureerd en gestandaardiseerd, maar kunnen onverwacht onderbroken worden door meldingen of signalen van cybercriminaliteit, bijvoorbeeld phishing, malware, DDoS aanvallen. Het uitvoeren van de werkzaamheden wordt gecompliceerd doordat hij/zij geconfronteerd wordt met een groeiende variatie aan vormen van online criminaliteit. Daardoor wordt van hem/haar een redelijke mate van alertheid en oplossingsgerichtheid verlangd, ondersteund door actuele kennis. Zo nodig moet de beginnend beroepsbeoefenaar zijn/haar kennisniveau van vormen van cybercriminaliteit en cyberveiligheid in een hoog tempo op peil brengen. Het afbreukrisico van de signaleringswerkzaamheden is hoog: wanneer hij/zij het werk niet tijdig of niet goed oplevert, heeft dat consequenties voor de veiligheid van collega's, processen, systemen en mogelijk zelfs klanten.

Verantwoordelijkheid en zelfstandigheid

De beginnend beroepsbeoefenaar voert het werk in een uitvoerende rol uit. Hij/zij werkt alleen maar ook samen met collega's. Hij/zij is verantwoordelijk voor de kwaliteit van het eigen werk. Hij/zij schakelt een collega of leidinggevende in als hulp nodig is of als de situatie daarom vraagt.

Vakkennis en vaardigheden

De beginnend beroepsbeoefenaar:

- heeft basiskennis van gedigitaliseerde criminaliteit (traditionele criminaliteit in een digitaal jasje) en cybercriminaliteit (middel en doel zijn digitaal), en het verschil daartussen
- heeft basiskennis van vormen van gedigitaliseerde criminaliteit, zoals cyberpesten, identiteitsfraude, phishing, marktplaatsfraude
- heeft basiskennis van vormen van cybercriminaliteit, zoals hacken, DDoS aanvallen, Malware, hergebruik van wachtwoorden
- heeft basiskennis van de manier waarop hackers te werk gaan (bijvoorbeeld de stappen van de Cyber kill chain)
- heeft basiskennis van verschillende typen hackers, zoals scriptkiddies, hacktivisten, vandalen/criminelen, georganiseerde cybercriminelen, staatshackers
- heeft basiskennis van de motieven van hackers, zoals digitale beroving, chantage, chaos veroorzaken, computer inzetten voor criminele activiteiten, status
- heeft basiskennis van de 7 beïnvloedingsprincipes van Social Engineering (Cialdini), zoals autoriteit, schaarste (op is op!), (geldelijk) gewin, en de toepassing daarvan door cybercriminelen
- heeft basiskennis van slimme apparaten die informatie kunnen bevatten die van nut kan zijn bij opsporing, bijvoorbeeld een slimme deurbel (met camera), een slimme thermostaat die het laatste tijdstip van beweging in een ruimte heeft vastgelegd
- heeft basiskennis van de digitale datadragers (apparaten) waarop sporen kunnen staan van gedigitaliseerde criminaliteit of cybercriminaliteit, zoals harde schijven, mobiele (smart) telefoons, tablet, USB sticks, SSD, CD/DVD, camera
- heeft basiskennis van de preventiemethoden voor cybercriminaliteit
- heeft basiskennis van het risicomanagementproces (identificeren, beoordelen, beheersmaatregelen in kaart brengen, risico's beheersen)
- heeft basiskennis van de te ondernemen stappen tegen cybercriminaliteit
- heeft kennis van organisaties en experts om in te schakelen als er sprake is van slachtofferschap bij zowel burgers als bedrijven

- kan betrouwbare bronnen over cybercriminaliteit en cyberveiligheid vinden en duiden
- kan vormen van gedigitaliseerde criminaliteit signaleren, bijvoorbeeld phishing mails, whatsapp fraude, neptelefoontjes / babbeltrucs
- kan vormen van cybercriminaliteit signaleren, bijvoorbeeld virussen, pop-ups, ransomware, clickbaits, valse webwinkels
- kan mogelijke risico's signaleren in een eenvoudige setting, bijvoorbeeld van een persoon of website van een sportvereniging
- kan de juiste hulpvraag stellen aan de juiste organisatie of expert
- kan een organisatie informeren over stappen in een risicomanagementproces (identificeren, beoordelen, beheersmaatregelen in kaart brengen, risico's beheersen)
- kan een organisatie informatie geven over maatregelen voor verbetering van de cyberveiligheid
- kan een organisatie informatie geven m.b.t. het veiligstellen van digitale sporen bij een cyberaanval

D1-K1-W1: Signaleert mogelijke risico's

Omschrijving

De beginnend beroepsbeoefenaar verzamelt informatie over de status van digitale beveiliging van een persoon, website of organisatie waar hij/zij werkt of waar hij/zij mee in aanraking komt tijdens het werk. Hij/zij vraagt bij de gebruiker/eigenaar van het systeem na of er aanwijzingen zijn van bedreigingen en checkt zelf in het systeem welke bedreigingen er zijn en welke kwetsbaarheden aanwezig zijn waar misbruik van gemaakt kan worden. Op basis hiervan formuleert hij/zij mogelijke risico's voor cyberaanvallen. Bij de uitvoering van de werkzaamheden overlegt hij/zij met collega's en/of leidinggevende.

Resultaat

Signalen van mogelijke risico's van cybercriminaliteit voor een persoon, website of (kleinere) organisatie zijn vastgelegd.

Gedrag

De beginnend beroepsbeoefenaar:
- checkt kritisch en accuraat de stand van zaken van de beveiliging op het gebied van techniek, de mens en organisatie;
- neemt initiatief in het stellen van vragen en stelt de juiste vragen en vervolgvragen om informatie te verkrijgen;
- vraagt actief de mening en ideeën van collega's en/of leidinggevende en luistert goed naar wat anderen naar voren brengen;
- beantwoordt vragen van anderen adequaat;
- legt de bevindingen kernachtig en volledig en op een logisch gestructureerde wijze vast;
- houdt zich aan voorgeschreven regels en procedures voor veilig werken en zorgvuldig handelen.

De onderliggende competenties zijn: Samenwerken en overleggen, Formuleren en rapporteren, Vakdeskundigheid toepassen, Onderzoeken, Instructies en procedures opvolgen

D1-K1-W2: Rapporteert over cyberveiligheid

Omschrijving

De beginnend beroepsbeoefenaar maakt een rapportage over de vormen van cybercriminaliteit en daarbij horende maatregelen voor cyberveiligheid die voor personen en organisaties relevant kunnen zijn. Eventueel raadpleegt hij/zij collega's of leidinggevende en vraagt hun mening en ideeën. Hij/zij informeert personen en organisaties door middel van de rapportage en mondelinge toelichting.

Resultaat

Rapportage over risico's voor cybercriminaliteit en mogelijke maatregelen voor cyberveiligheid voor een persoon, website of organisatie is gemaakt (opgeleverd) en aangeboden.

Gedrag

De beginnend beroepsbeoefenaar:
- rapporteert feitelijk, volledig en nauwkeurig over de stand van zaken van de digitale beveiligingssituatie en mogelijke maatregelen voor cyberveiligheid;
- komt zelf actief met ideeën, standpunten en/of voorstellen, geeft illustratieve voorbeelden en onderbouwt met steekhoudende argumenten;
- licht de rapportage helder toe;
- luistert aandachtig naar de mening of ideeën van collega's en/of leidinggevende en vraagt door op wat de ander vertelt;
- luistert aandachtig naar vragen, beantwoordt vragen adequaat en geeft heldere aanvullende informatie;
- stelt logische vragen en vervolgvragen om te checken of de rapportage helder is;
- handelt professioneel en integer.

De onderliggende competenties zijn: Aandacht en begrip tonen, Overtuigen en beïnvloeden, Formuleren en rapporteren, Vakdeskundigheid toepassen