Examenopdrachten

P2-K2 Security

Algemene informatie		
Examenvorm	Examenproject - Praktijkexamen in een gesimuleerde omgeving	
Kwalificatiedossier en cohort	IT systems and devices	2020 en verder
Profiel, niveau en crebocode	P2: Expert IT systems and devices, niveau 4	25606
Kerntaak	P2-K2: Controleert de security	
Werkprocessen	P2-K2-W1: Geeft security advies en verbetert de security P2-K2-W2: Reageert op security incidenten	
Examenduur	6 uur (eventuele pauzes niet meegerekend)	

Opdracht 1: Adviseren en verbeteren security

3 uur (180 minuten)

Situatie

Op jullie ROC hebben ze een Bring Your Own Device (BYOD) beleid. Dit betekend dat de student en bezoekers hun eigen device, vaak laptops, meenemen naar de studie. Voor dit beleid hebben ze nog geen regels opgesteld om hun netwerkomgeving veilig te houden. De dienst ICT (opdrachtgever) van jouw ROC wil dat de studenten een veilig netwerkomgeving hebben en eist daardoor een erkend anti viruspakket zoals AVG, ESET of Kaspersky. Dienst ICT wil dat jij de juiste antivirustool kiest en motiveert waarom jij de antivirus hebt gekozen. Dienst ICT heeft verder wel wat eisen aan waar het pakket aan moet voldoen, de eisen vind je in de opdracht terug. Daarnaast willen ze in hetzelfde rapport, advies hebben over hoe vaak en wanneer een back-up en updates gedraaid moeten worden.

Opdracht

1. Maak een memo naar Dienst-ICT waarin je het volgende omschrijft:
    a. Zoek de juiste antivirustool en motiveer waarom je hiervoor hebt gekozen. Deel hierbij ook je vergelijkingssheet, bijvoorbeeld via een vergelijkingssite.
    b. Omschrijf de volgens jou 'beste back-up methode'. Hierin omschrijf je met welke methode en hoe vaak je een back-up maakt. Tevens omschrijf je waar je deze back-up plaatst (denk bijvoorbeeld aan on- of off-site, USB, NAS etc.) én waar je verder aan moet denken bij het wegschrijven van een beveiligde back-up.
    c. Als laatst geef je advies over de updates; welke zijn belangrijk, welke zijn verplicht en hoe test je bijvoorbeeld voordat je de updates uitrolt.

2. Verwerk bovenstaande in de *bijlage 1.0 - Memo dienst-ICT.*

Voorbereiden

Neem de bovenstaande situatie goed door.

Uitvoeren

1. Je krijgt als opdracht eventuele veiligheidslekken en/of kwetsbaarheden op te sporen binnen een IT-omgeving. Je schrijft hiervoor een plan, waarin je omschrijft welke tools je gebruikt en welke onderdelen je daarmee gaat testen.
2. Geef aan welke kwetsbaarheden en bedreigingen jij verwacht te vinden.
3. Stel verbetervoorstellen op voor de bestaande situatie.
4. Communiceer je bevindingen met betrokken personen. Dit gebeurt digitaal. Motiveer je gemaakte keuzes in de e-mail in *bijlage 2.0 – e-mail aan opdrachtgever.*

Resultaat

Als resultaat van deze opdracht lever je de volgende producten en/of diensten op.

- De memo (verslag) aan de opdrachtgever (Bijlage 1.0)
- Word document met de mail als inhoud aan de opdrachtgever (Bijlage 2.0)

Bijlagen

Bijlage	Vindplaats
Bijlage 1.0 – Memo dienst-ICT	Map Digitale bijlagen
Bijlage 2.0 – E-mail aan opdrachtgever	Map Digitale bijlagen

Opdracht 2: Reageren op security incidenten

3 uur (180 minuten)

Situatie

Via de servicedesk komt een incident binnen, een BYOD-laptop is met malware overgenomen. De betreffende collega had een bestelling gedaan bij een bekende webwinkel en had hiervoor vanuit de e-mail een link aangeklikt om zo extra korting te ontvangen. Helaas was dit geen betrouwbare link en werd de laptop volledig geblokkeerd.

De bestanden op de laptop zijn opgeslagen op de gedeelde netwerkschijf waar deze collega toegang toe heeft. Deze bestanden lijken ook geëncrypt te zijn. Vrijgeven lijkt volgens een gevonden bestand op het bureaublad alleen mogelijk d.m.v. een crypto-betaling.

Opdracht

Je gaat reageren op security incidenten.

Uitvoeren

1. Detecteer en analyseer (een) security incident(en).
2. Schat de prioritering en omvang van het incident in.
3. Beschrijf een oplossing om het incident te bestrijden/de schade te beperken. Denk hierbij aan de memo uit opdracht 1.
4. Verwerk je handelingen in een logboek (bijlage 4.0 – Logboek dienst ICT) (stap voor stap) conform de procedures (AVG) van de organisatie (zie bijlage 5.0 – AVG voor medewerkers).
5. Koppel de afhandeling terug aan de betrokkenen door middel van een mail (bijlage 3.0 – E-mail betrokkenen).

Resultaat

Als resultaat van deze opdracht lever je de volgende producten en/of diensten op.

- Een logboek
- De communicatie met betrokken personen/instanties
- Word document met de mail als inhoud aan de opdrachtgever.

Bijlagen

Bijlage	Vindplaats
Bijlage 3.0 – E-mail aan betrokkenen	Map Digitale bijlagen
Bijlage 4.0 – Logboek dienst ICT	Map Digitale bijlagen
Bijlage 5.0 – AVG voor medewerkers	Map Digitale bijlagen

Einde examenproject

Lever alle resultaten, de examenopdrachten, gebruikte bijlagen en de eventuele materialen in bij de examinator.