M1 Challenge: Cybersecurity Debat

Doel

Je bereidt je als groep voor op het einddebat waarin je individueel stelling neemt en argumenteert over een belangrijk cybersecuritythema. Tijdens het debat wordt niet alleen gekeken naar jullie kennis, maar vooral naar hoe goed jullie die kennis kunnen toepassen, beargumenteren en koppelen aan concrete voorbeelden.

De challenge-opdracht bereid je voor op het einddebat, waarin je aantoont dat je begrip hebt ontwikkeld op de volgende thema's:

1. **Impact van incidenten:** Wat de concrete gevolgen zijn van cybersecurity-incidenten voor individuen, organisaties en de maatschappij.
2. **Maatregelen en afwegingen:** Welke maatregelen er zijn (technisch, organisatorisch, juridisch, mensgericht) en welke keuzes en trade-offs organisaties daarbij maken.
3. **Governance en organisatie:** Hoe cybersecurity structureel georganiseerd kan worden binnen organisaties (rollen, beleid, ISMS, normen en wetgeving).
4. **Acceptatie en weerstand:** Waarom cybersecurity nog vaak onvoldoende prioriteit krijgt of weerstand oproept (bijv. kosten, gebruiksgemak, onzichtbare waarde), en hoe dit kan worden doorbroken.
5. **Bedreigingen en risico-inschatting:** Welke dreigingen relevant zijn, hoe waarschijnlijk ze zijn, en hoe organisaties hun risico's kunnen verkleinen.
6. **Balans en overtuigingskracht:** Hoe je overtuigend beargumenteert waarom cybersecurity geen "bijzaak" is, maar een randvoorwaarde voor continuïteit en vertrouwen in de samenleving.

Bronnen

Bronnen waar je eventueel kan starten met het onderzoek:

- https://www.nctv.nl/onderwerpen/c/cybersecuritybeeld-nederland
- https://www.nctv.nl/onderwerpen/n/nationaal-cyber-security-centrum
- https://www.enisa.europa.eu/publications/2024-report-on-the-state-of-the-cybersecurity-in-the-union (https://www.enisa.europa.eu/)
- https://www.nist.gov/cyberframework
- https://atwork.safeonweb.be/tools-resources/cyberfundamentals-framework
- https://www.nu.nl/economie/6368261/gasten-van-der-valk-hotels-opgelicht-doordat-medewerkers-op-phishinglink-klikten.html
- Kijk ook op de bibliotheek van BrightSpace

Opdrachtomschrijving

Jullie werken met de studiegroep aan deze opdracht. In dit debat moeten jullie aantonen dat je de technische, organisatorische, menselijke en maatschappelijke dimensie van cybersecurity begrijpen. Cybersecurity is immers niet vanzelfsprekend: het wordt nog vaak gezien als een kostenpost, lastig of beperkend voor de gebruiker. Jullie uitdaging is om te laten zien dat cybersecurity juist een noodzakelijke voorwaarde is voor vertrouwen, continuïteit en innovatie – en dat dit overtuigend kan worden beargumenteerd. Dat cybersecurity wel vanzelfsprekend zou moeten zijn!

Samen verdiepen jullie jezelf in de volgende thema's en verwerken dit in groepsdossier:

1. **Gevolgen van incidenten**
    a. Welke impact hebben incidenten op individuen (privacy, financiële schade, reputatie)?
    b. Welke impact op organisaties (continuïteit, juridische claims, reputatieverlies)?
    c. Welke impact op de maatschappij (vertrouwen in digitale systemen, afhankelijkheid van technologie, publieke veiligheid)?
    d. Opdracht: verzamel minimaal drie echte incidenten (uit de actualiteit) en analyseer de gevolgen voor elk van deze drie niveaus. Beschrijf niet alleen de schade, maar ook de indirecte effecten (vertrouwen, reputatie, psychologische impact).
2. **Maatregelen**
    a. Onderzoek welke soorten maatregelen zijn er? (technisch, organisatorisch, procesmatig, mensgericht).
    b. Weeg af: welke kosten, beperkingen of weerstand kunnen maatregelen oproepen? Waarom kiezen organisaties soms níet voor de veiligste optie?
    c. Welke maatregelen zijn effectief tegen jullie gekozen incidenten?
    d. Opdracht: kies per incident minimaal 2 maatregelen en leg uit waarom die passend zijn, en welke trade-offs er zijn (kosten, gebruiksgemak, cultuur).
3. **Cybersecurity governance**
    a. Hoe organiseer je cybersecurity in een organisatie?
    b. Wat is de rol van beleid, normen (ISO27001/27005), wetgeving (AVG, NIS2) en het ISMS?
    c. Laat zien hoe governance kan helpen om maatregelen breed geaccepteerd en ingebed te krijgen.
    d. Opdracht: maak een korte schets van hoe jullie denken dat Avans Hogeschool (of een ander concreet voorbeeld uit de praktijk) cybersecurity governance kan verbeteren.

4. **Weerstand en Acceptatie**
    a. Breng in kaart waarom medewerkers, management of klanten cybersecuritymaatregelen niet altijd accepteren.
    b. Denk aan factoren als: kosten, gemak vs. veiligheid, cultuur, communicatie, of gebrek aan urgentiebesef.
    c. Opdracht: Gebruik hiervoor ten minste 2 praktijkvoorbeelden (bijv. uit nieuws of uit eigen ervaring binnen Avans, werk of bijbanen).
5. **Acceptatie**
    a. Zoek en beschrijf manieren waarop organisaties weerstand kunnen verminderen en acceptatie kunnen vergroten.
    b. Opdracht: Vergelijk minimaal 2 verschillende strategieën en beoordeel welke volgens jullie het meest effectief zijn.
6. **Bedreigingen & kansen**
    a. Welke actuele dreigingen zijn er? (phishing, ransomware, insider threats, AI misbruik, etc.).
    b. Hoe groot is de kans dat een organisatie geraakt wordt door deze dreigingen? Hoe kan je die kans reduceren?
    c. Opdracht: kies 3 dreigingen en maak een inschatting van hun waarschijnlijkheid en impact. Onderbouw dit met bronnen en argumenten.

Werkwijze

Iedere student neemt de lead op ten minste één thema (1 t/m 6). Je werkt als lead aan het thema met meerdere studenten van jouw groep. Bij het bespreken van het resultaat in de groep, vervullen de andere studenten de rol van “debattrainers” door kritische vragen te stellen. Bijvoorbeeld “Waarom zou een bedrijf dit doen?” of “Wat als de maatregel te duur is?”.

Jullie maken een groepsdossier (max. 12 pagina’s) met analyses, voorbeelden en argumenten. Dit dossier dient als basis voor jullie voorbereiding op het debat en mag je op de dag van het debat gebruiken ter ondersteuning. In het dossier is zichtbaar dat jullie werken met:

- Gevolgenanalyses van incidenten
- Overzicht van maatregelen en trade-offs
- Voorstel voor governance en organisatie
- Analyse van acceptatie & weerstand
- Dreigingsanalyse

Neem dit dossier op in jouw portfolio en schrijf jouw leeruitkomst (reflectie) hierop. Beantwoord hier de volgende vragen:

- Wat heb je geleerd?
- Wat vond je verassend?
- Wat vind je lastig?
- Waar wil je nog aan werken?