KEUZEMODULE CYBERSECURITY
WEERBAAR TEGEN CYBERCRIME

Module 1 - Wat is cybersecurity en cybercrime?

Workshop 1 – De wereld van cybercrime

avans hogeschool

LEERUITKOMST MODULE 1

Je hebt een fundamenteel begrip van cybersecurity en bent met een risico-bewuste mentaliteit in staat om wet- en regelgeving, risicomanagement en het beheer van cybersecurity toe te passen in een organisatie, zodanig dat daarmee effectief wordt bijgedragen aan het beveiligingsbeleid en risicobeheer binnen organisaties.

avans hogeschool

MODULE CYBERSECURITY

Overzicht

Week 1: Risicodenken

- Workshop 1: De wereld van cybercrime
- Workshop 2: Risicodenken en -management
- Workshop 3: Governance van cybersecurity

Week 2: Risicoanalyse

- Workshop 4: Risico-assessment
- Workshop 5: Beveiligingsmaatregelen

Week 3: Challenge, uitstapje en afronding

WAARMEE GA JE VANDAAG AAN DE SLAG?

Leeruitkomst workshop

- Je begrijpt wat wordt verstaan onder cybercriminaliteit.
- Je hebt een dieper inzicht in hedendaagse cyberdreigingen, de impact ervan op organisaties en waarom cybersecurity cruciaal is voor moderne organisaties. Door het analyseren van dreigingsbeeld rapporten kun je de motieven van cybercriminelen begrijpen, de potentiële dreigingen voor verschillende soorten organisaties identificeren en de waarde van cybersecurity inzien.

AGENDA WORKSHOP 1

- Gastcollege Peter Lahousse

- Historisch perspectief
- Definities
- Taxonomie van cybercriminaliteit
- Soorten criminelen en hun motieven

- Opdracht
- Tips voor bronnen

PETER LAHOUSSE

Oprichter **Cybercrimeinfo.nl**

Abonneer op de nieuwsbrief!

Expert in Cybercriminaliteit en Darkweb Opsporing
Cybersecurity Trainer &
Bewustwordingsadviseur
Innovator in Digitale Veiligheid

avans hogeschool

CYBERCRIME IN HISTORISCH PERSPECTIEF

- 1970 – 1990

  Komst internet en e-mail. Phone phreaken, virussen

- 1990 – 2000

  Toename gebruik internet. Virussen, Remote Access Tools

- 2000 – 2010

  Verdere ontwikkeling internet en computercriminaliteit, door opkomst internetdiensten, online markten

- 2010 – 2020

  Opkomst darknet markets, aanvallen door statelijke actoren

- 2020 – 2025 ?

EEN PAAR DEFINITIES

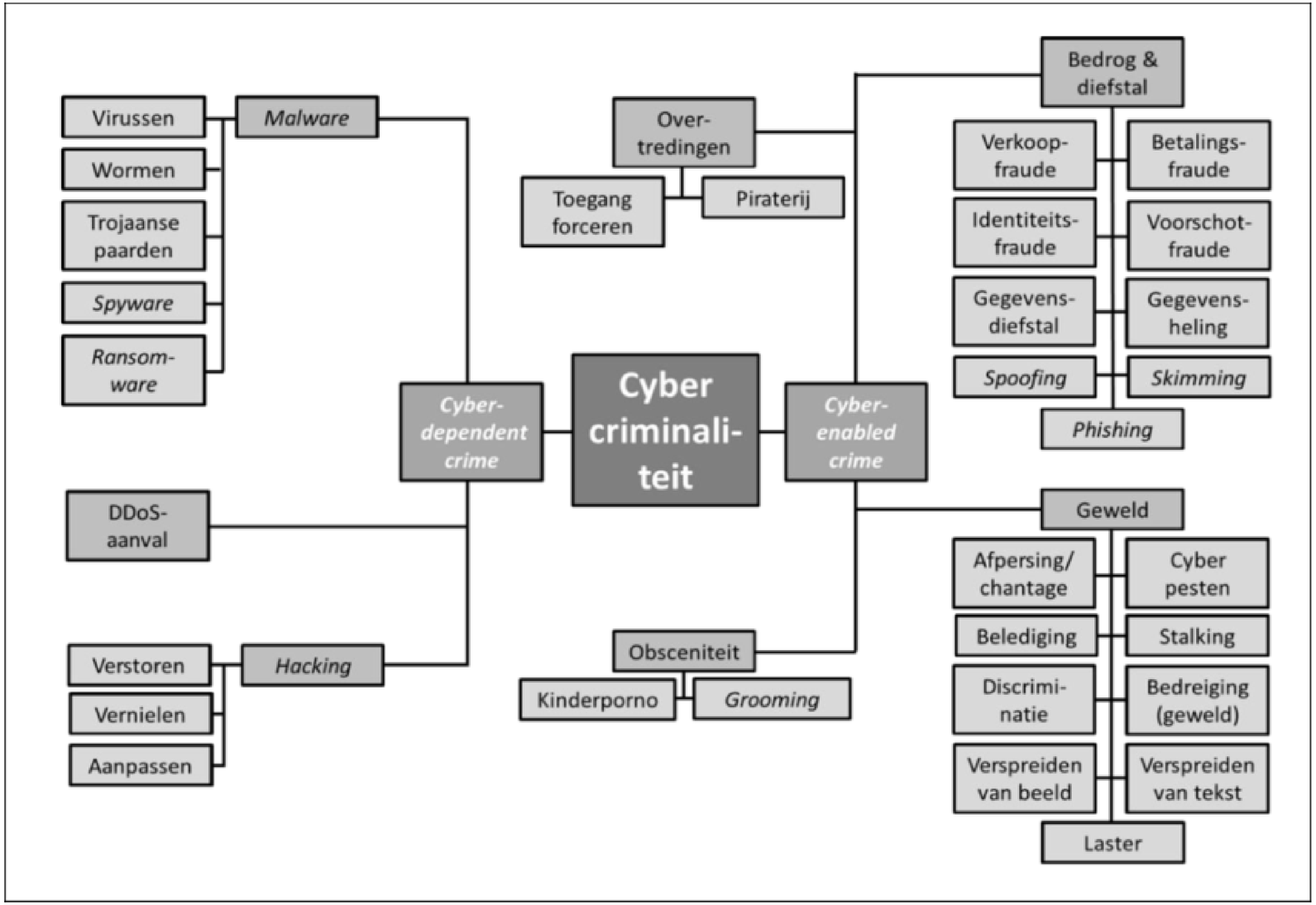
Cybercriminaliteit in enge zin

Strafbare gedragingen waarbij computers en netwerken zowel het doelwit als het middel zijn van criminaliteit. Gedragingen die integriteit, beschikbaarheid en exclusiviteit van gegevens in computers aantasten. Nieuwe delicten die in het verleden nog niet bestonden.

Cybercriminaliteit in ruime zin, ofwel gedigitaliseerde criminaliteit

Criminaliteit waarbij computers en internet als instrument worden gebruikt om traditionele criminaliteit te plegen.

TAXONOMIE VAN CYBERCRIMINALITEIT



SPITHOVEN, R. (2020). VERBONDEN RISICO'S: MAATSCHAPPELIJKE VEILIGHEID IN DE BLACK BOX SOCIETY. DEN HAAG: BOOM CRIMINOLOGIE.

WIE EN WAAROM?

Typen daders

- Overheden (statelijke actoren)
- Terroristen
- (Goed georganiseerde) criminele organisaties
- Beroepscriminelen
- Hacktivisten
- Insiders
- Gemotiveerde individuen
- Cybervandalen / scriptkiddies

Motieven

- Intellectueel
- Sensatie-gerelateerd
- Status-gerelateerd
- Financieel
- Wraakzuchtig
- Ideologisch

GROEPSOPDRACHT:
WAAROM IS CYBERSECURITY BELANGRIJK VOOR ORGANISATIES?

Doel: Een dieper inzicht krijgen in cyberdreigingen, de impact ervan op organisaties en waarom cybersecurity cruciaal is voor moderne organisaties. Door het analyseren van dreigingsbeeld rapporten kun je de motieven van cybercriminelen begrijpen, de potentiële dreigingen voor verschillende soorten organisaties identificeren en de waarde van cybersecurity inzien.

Ga als volgt te werk:

1. Selecteer twee recente dreigingsbeeld rapporten van een betrouwbare bron, zoals een overheidsinstantie, cybersecuritybedrijf of onderzoeksinstituut. Eén rapport uitgegeven door een Nederlandse (overheids)instantie en één rapport uitgegeven op internationaal niveau.

2. Analyseer de rapporten grondig en identificeer de belangrijkste dreigingen die worden beschreven. Gebruik de volgende vragen als leidraad voor jullie analyse:
   a. Welke soorten organisaties worden het meest getroffen door deze dreigingen en waarom?
   b. Wat zijn de belangrijkste motieven van cybercriminelen zoals beschreven in het rapport?
   c. Hoe kunnen deze dreigingen de operationele activiteiten van een organisatie beïnvloeden?
   d. Zijn er trends of patronen in de doelwitten of methoden van aanval die worden benadrukt in het rapport?

3. Werk samen als groep om jullie bevindingen te bespreken en een samenvatting van het beeld op te stellen, vormgegeven als een infographic. Geef daarin antwoord op de vraag: waarom is cybersecurity belangrijk voor organisaties?

4. **Een aantal groepen zal hun uitkomsten morgenochtend presenteren in min. 5 en max. 10 minuten voor de klas.**

BRONNEN
(NOOIT VOLLEDIG, GA OOK ZELF OP ZOEK!)

- Zie Bibliotheek op Brightspace

Bijvoorbeeld:

- https://www.aivd.nl/onderwerpen/cyberdreiging/aivd-publicaties-over-cyberdreiging
- https://www.nctv.nl/onderwerpen/cybersecuritybeeld-nederland
- https://www.isc2.org/-/media/Project/ISC2/Main/Media/Marketing-Assets/Reports/2023_CDR_Report_FINAL2_ISC2.pdf
- https://www.rathenau.nl/nl/digitalisering/online-ontspoord
- https://www.enisa.europa.eu/publications/foresight-cybersecurity-threats-for-2030-update-2024-extended-report