KEUZEDELEN

edu actief

BASIS CYBERCRIMINALITEIT EN CYBERVEILIGHEID

Boom beroepsonderwijs

COLOFON

Boom beroepsonderwijs
info@boomberoepsonderwijs.nl
www.boomberoepsonderwijs.nl

Auteur: Jan Dolphijn

Titel: Basis cybercriminaliteit en cyberveiligheid

ISBN: 978 90 372 6426 5

Bronvermelding: Martijn van der Voo

Eerste druk/ eerste oplage

INHOUD

WERKEN MET DIT KEUZEDEEL

Digitale leeromgeving

Bij sommige opdrachten heb je hulpmiddelen nodig, bijvoorbeeld filmpjes, formulieren of een link naar een website. Deze staan allemaal in de digitale leeromgeving. Het icoontje in de vorm van een wereldbol verwijst naar de digitale leeromgeving. Om hier te komen ga je naar digitaal.boomonderwijs.nl/beroepsonderwijs.

Eerste keer inloggen in de digitale omgeving
Voordat je de digitale leeromgeving kunt gebruiken, moet je je licentie activeren.

- Overleg met je docent welk type account je gebruikt.
- Ga naar www.boomberoepsonderwijs.nl/licentie.
- Bekijk de instructiefilm of lees het stappenplan.
- Volg de stappen.

Daarna kun je aan de slag!

Basis cybercriminaliteit en cyberveiligheid
Als beveiliger binnen een organisatie ben je je constant bewust van de omstandigheden waarin jij je bevindt. Je hebt je ogen en oren open, staat in contact met je collega's en weet wanneer een situatie dreigend wordt of kan escaleren. Tijdens je opleiding leer je alert te zijn op het gedrag van mensen, en hoe te handelen bij incidenten. Je bent hulpvaardig en dienstverlenend naar personeel en burgers en weet je collega's aan te sturen. Kortom, je bent een bekwame beveiliger of wordt hiervoor opgeleid. In dit keuzedeel leer je de belangrijkste vormen van cybercriminaliteit kennen. Je kunt niet alleen menselijke dreigingen, maar ook digitale dreigingen herkennen.

Het doel van dit keuzedeel is je kennis te laten maken met de dreigingen en kwetsbaarheden van de digitale wereld, die je tijdens je werk kunt tegenkomen. Je leert risico's te herkennen en actie te ondernemen als er een digitaal incident dreigt of in uitvoering is. Je leert over je bevindingen te communiceren en deze in een rapportage vast te leggen.

Bekijk het filmpje en bedenk wat jij zou doen.

Leerdoelen

1. heeft basiskennis van gedigitaliseerde criminaliteit (traditionele criminaliteit in een digitaal jasje) en cybercriminaliteit (middel en doel zijn digitaal), en het verschil daartussen
2. heeft basiskennis van vormen van gedigitaliseerde criminaliteit, zoals cyberpesten, identiteitsfraude, phishing, Marktplaats-fraude
3. heeft basiskennis van vormen van cybercriminaliteit, zoals hacken, DDoS-aanvallen, malware, hergebruik van wachtwoorden
4. heeft basiskennis van de manier waarop hackers te werk gaan (bijvoorbeeld de stappen van de cyber kill chain)
5. heeft basiskennis van verschillende typen hackers, zoals script-kiddies, hacktivisten, vandalen/criminelen, georganiseerde cybercriminelen, staatshackers
6. heeft basiskennis van de motieven van hackers, zoals digitale beroving, chantage, chaos veroorzaken, computer inzetten voor criminele activiteiten, status
7. heeft basiskennis van de zeven beïnvloedingsprincipes van social engineering (Cialdini), zoals autoriteit, schaarste (op is op!), (geldelijk) gewin, en de toepassing daarvan door cybercriminelen

8. 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
9. heeft basiskennis van de digitale datadragers (apparaten) waarop sporen kunnen staan van gedigitaliseerde criminaliteit of cybercriminaliteit, zoals harde schijven, mobiele (smart) telefoons, tablets, USB-sticks, SSD's, cd/dvd's, camera's
10. heeft basiskennis van de preventiemethoden voor cybercriminaliteit
11. heeft basiskennis van het risicomanagementproces (identificeren, beoordelen, beheersmaatregelen in kaart brengen, risico's beheersen)
12. heeft basiskennis van de te ondernemen stappen tegen cybercriminaliteit
13. heeft kennis van organisaties en experts om in te schakelen als er sprake is van slachtofferschap bij zowel burgers als bedrijven
14. kan betrouwbare bronnen over cybercriminaliteit en cyberveiligheid vinden en duiden
15. kan vormen van gedigitaliseerde criminaliteit signaleren, bijvoorbeeld phishingmails, whatsappfraude, neptelefoontjes/babbeltrucs
16. kan vormen van cybercriminaliteit signaleren, bijvoorbeeld virussen, pop-ups, ransomware, clickbaits, valse webwinkels
17. kan mogelijke risico's signaleren in een eenvoudige setting, bijvoorbeeld van een persoon of website van een sportvereniging
18. kan de juiste hulpvraag stellen aan de juiste organisatie of expert
19. kan een organisatie informeren over stappen in een risicomanagementproces (identificeren, beoordelen, beheersmaatregelen in kaart brengen, risico's beheersen)
20. kan een organisatie informatie geven over maatregelen voor verbetering van de cyberveiligheid
21. kan een organisatie informatie geven met betrekking tot het veiligstellen van digitale sporen bij een cyberaanval.

Dit keuzedeel bestaat uit:

- *Theorie, begrippen en opdrachten*
  Hierbij leer je over en oefen je met de praktijk. In sommige opdrachten werk je aan beroepsproducten, deze opdrachten herken je aan [BP]. Deze beroepsproducten kun je verzamelen in je portfolio en je hebt ze nodig om de uitdaging aan het einde van het keuzedeel goed af te ronden.
  De beroepsproducten in dit keuzedeel zijn:
  - *Ransomware*
  - *Casus Melding van identiteitsfraude*
  - *Insiders bij 'het bedrijf'*
  - *Casus Acceptabel gebruik*

- *Test je kennis*
  Hiermee kun je zelf je kennis van de theorie testen.

- *Uitdaging*
  Dit is het eindproduct en de afronding van het keuzedeel. Hier werk je gedurende het hele keuzedeel naartoe. En hier word je op beoordeeld.
  Voor de uitdaging van dit keuzedeel word je meegenomen in een aantal praktijksituaties waarin je mogelijke cyberdreiging herkent, de juiste stappen neemt en hier correct over rapporteert.

- *Theorietoets*
  Je docent besluit of je ter afsluiting een theorietoets maakt.

HOOFDSTUK 1
CYBERCRIMINALITEIT

In dit hoofdstuk maak je kennis met de meest voorkomende vormen van cybercriminaliteit. Je krijgt telkens een stukje theorie, een praktische opdracht en een korte herhalingstoets. Over deze vormen van cybercrime krijg je informatie:

- malware
- phishing
- spam
- identiteitsdiefstal
- datalekken
- insiders.

Aan het eind van dit hoofdstuk

1. weet je wat cyberdreigingen in de beroepsomgeving zijn en kun je preventieve maatregelen voorstellen
2. kun je je bevindingen naar collega's en leidinggevenden communiceren
3. ken je de mogelijke risico's en kun je dit vastleggen in rapportage.

Opdracht 1 Heb jij wat te verbergen?

Bekijk het filmpje en de website.

Heb jij wat te verbergen, denk je? Zo ja, waarom?

Malware

Handhavers maken onderscheid tussen cybercriminaliteit en gedigitaliseerde criminaliteit. Het verschil is dat cybercriminaliteit een misdrijf is dat wordt gepleegd met als doel het stelen van digitale data of het platleggen van een digitaal systeem. De middelen en het doelwit zijn digitaal. Bij gedigitaliseerde criminaliteit wordt gebruikgemaakt van een ICT-middel.

Neem bijvoorbeeld het bekende stelen van gevoelig fotomateriaal van iemands telefoon. Je doet dit met je computer, je richt je op de mobiele telefoon van het slachtoffer en ook de 'buit', de foto's, is digitaal. Dit is een voorbeeld van **cybercriminaliteit**: middel en doelwit zijn digitaal.

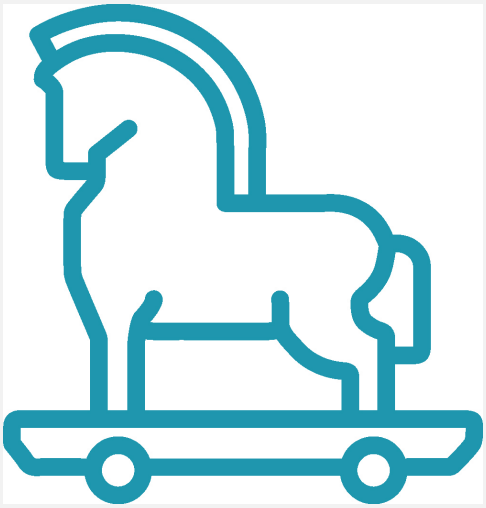
Bij **gedigitaliseerde criminaliteit** wordt gebruikgemaakt van een ICT-middel om een misdrijf te plegen. Heb je weleens Marktplaats-fraude meegemaakt? Daarbij word je voor geld opgelicht en krijg je geen spullen, of iets totaal anders dan je dacht. De bedrieger maakt gebruik van een digitaal middel om iemand op te lichten. Een ander voorbeeld is dat een onverlaat het dark web gebruikt om drugs te kopen en deze via social media gaat verkopen. Die persoon gebruikt digitale middelen om misdrijven te plegen, in dit geval drugs verkopen.

In de praktijk zijn deze vormen van criminaliteit vaak lastig van elkaar te onderscheiden. Voor jou als beveiliger kan het van belang zijn te weten met welke vorm je te maken hebt. Je kunt bij een digitaal incident dan een betere inschatting maken hoe je je leidinggevende kunt informeren of welke specialist je het best kunt inschakelen.

Malware

De term malware is een samenvoeging van *malicious* en *software* (kwaadaardige software). Malware is een verzamelterm voor honderdduizenden soorten software, gemaakt om de werking van informatiesystemen te verstoren of ongeoorloofd toegang te krijgen tot een systeem. Malware wordt heimelijk aan het doelsysteem toegevoegd en voert vaak onopgemerkt ongewenste taken uit. Malware kent tienduizenden varianten, waarvan trojans en virussen de bulk vormen.

Bedenk dat malware op alle systemen voorkomt, op computers maar vooral ook op Android toestellen, laptops en telefoons. iPhones blijken er wat beter tegen bestand, maar er zijn inmiddels voorbeelden te vinden waarbij ook de iPhone besmet is geraakt.



Trojan horse

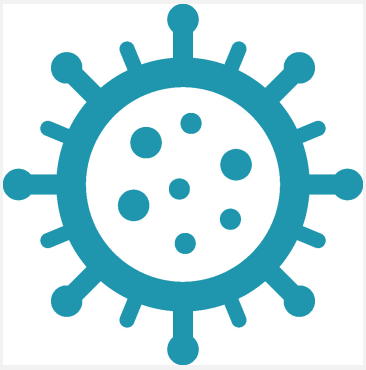
Een trojan horse is een computerbestand dat zich voordoet als iets nuttigs en wenselijks. Echter, onder de bovenlaag voert de trojan onverwachte en ongeautoriseerde (= ongeoorloofd, zonder toestemming) taken uit. Dit verklaart meteen de naam: het houten paard van Troje was een geschenk, maar eenmaal de stad binnengereden bleek het vijandige soldaten in zich te herbergen. Een voorbeeld is een app downloaden die niet in de Playstore staat, maar bijvoorbeeld op een forum. Na het installeren blijkt het om een virus te gaan.

De gebruiker plaatst vrijwillig de software op het eigen systeem. Ook hier gaat de vergelijking met Troje op, want de inwoners haalden het paard uit nieuwsgierigheid naar binnen. Hoe beter de trojan zich voordoet als echt, hoe succesvoller het bestand de ongeoorloofde taken kan uitvoeren.

De meest gebruikte trojans zijn:

- **backdoor trojans**
  Dit type trojan is door een hacker op een systeem geplaatst, zodat de hacker toegang krijgt tot dit systeem. Die persoon kan zelf bijvoorbeeld in China zitten. Je ziet hier dus niets van, maar er is wel een verbinding.
- **downloader trojans**
  Dit type trojan kopieert software naar het doelsysteem. Meestal gaat het om ongewenste apps (adware) of andere misleidende software. De downloader trojan heeft geen backdoor naar buiten en de hacker heeft geen directe toegang tot het systeem.
- **DDoS trojans**
  Dit type trojan installeert malware waarmee DDoS attacks kunnen worden uitgevoerd. De besmette computer wordt onderdeel van een botnet. DDoS en botnets worden verderop uitgelegd.
- **bank trojans**
  Dit is een veelvoorkomende trojan met als functie het stelen van bankgegevens, vaak door middel van phishingtechnieken. Deze trojan installeert software waarmee toetsenbordaanslagen kunnen worden gelezen, of zoekt op je systeem naar inloggegevens.

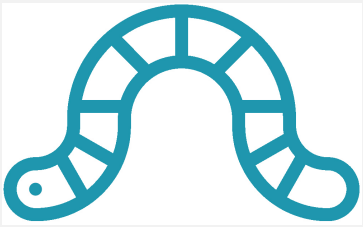
Virus



Een computervirus is een programma dat ongeautoriseerde acties uitvoert op een informatiesysteem. Een virus onderscheidt zich van andere malware doordat het zichzelf kan activeren en repliceren. Een virus koppelt zich aan een app en zodra de app wordt gestart, wordt ook het virus actief.

Het eerste bekende virus is ‘creeper’ uit 1971. In de loop der jaren zijn er tienduizenden virussen ontwikkeld in allerlei verschijningsvormen, waarvan er hier enkele worden beschreven:

- **resident virus**
  Iedere keer als de computer opstart, wordt het virus actief.
- **niet-resident virus**
  Eenmaal gestart zoekt dit virus actief naar bestanden die het ook kan besmetten. Als het een andere app heeft besmet, verwijdert het zichzelf uit het geheugen.
- **polymorf virus**
  Polymorfe virussen veranderen zichzelf iedere keer dat het virus een ander bestand besmet. Daardoor kan de virusscanner van een computer het niet ontdekken.
- **metamorf virus**
  Dit is een zeer geavanceerd virus, dat zich aan appjes koppelt en dan zichzelf zo verandert dat het van je Windows computer kan overspringen naar je Android telefoon. Het is heel moeilijk op te sporen.



Worm

Een worm verspreidt zich via het netwerk naar andere systemen. Anders dan een virus heeft een worm geen app nodig. Een worm maakt een app met een kopie van zichzelf en stuurt deze vervolgens naar ander systemen. Dit kan via e-mail of andere verbindingen, zoals chats of games. Wormen zijn vrijwel zonder menselijke tussenkomst actief. Het enige wat de gebruiker hoeft te doen, is een geïnfecteerd appje of document te openen en de worm kan zich al verspreiden. De meest bekende vormen zijn:

- **e-mailwormen**
  Deze worden verspreid via bijlagen in e-mailberichten.
- **internetwormen**
  Deze verspreiden zich over het internet door misbruik te maken van een slechte beveiliging op het doelsysteem.
- **netwerkwormen**
  Deze verspreiden zich door zichzelf te kopiëren naar slecht beveiligde systemen in het eigen netwerk.

Ransomware

Naar alle waarschijnlijkheid vormt ransomware anno 2022 de grootste bedreiging op het gebied van malware-infecties in Nederland. De kwaadaardige app maakt alle bestanden op een computer onleesbaar. Dit kan alleen ongedaan gemaakt worden als er een sleutel wordt ingevoerd. Die sleutel moet worden gekocht bij de criminelen en uiteraard is volstrekt onzeker of je je bestanden ooit weer leesbaar krijgt. De versleuteling kan niet worden gebroken, want de manier waarop wordt versleuteld is te krachtig voor een gebruiker om dit zelf te kunnen doen.

Een goede bescherming is om belangrijke bestanden altijd naar een cloudoplossing te kopiëren. Gebruik Dropbox, OneDrive of Google Drive (alle drie gratis) om de bestanden op het systeem veilig te houden. Als je systeem besmet raakt, heb je wel overlast, maar je bent geen data kwijt. Het systeem leegmaken en weer opnieuw installeren is een tijdrovende bezigheid, echter veel minder schadelijk dan het verlies van je data!

Malwaretrends

De afgelopen jaren zijn enkele nieuwe vormen van malware actief geworden. De bekendste is **ransomware**. Deze software maakt data op het systeem onleesbaar en alleen na betaling kun je dit weer ongedaan maken. Ransomware is sinds 2018 regelmatig in het nieuws geweest vanwege de spectaculaire impact die het heeft op bedrijven, overheidsinstanties en andere instellingen.

Volgens grote beveiligingsbedrijven als Kaspersky, Microsoft, Symantec en Trend Micro Fileless is malware veruit de meest voorkomende dreiging op alle apparaten en besturingssystemen. Malware staat al jaren vermeld als belangrijkste dreiging voor systemen in bedrijven.

Opdracht 2 Controle virusscanner

Om de actieve werking van je virusscanner te controleren op je Windows 10 of 11 computer kun je gebruikmaken van het EICAR testvirus. Het EICAR virus is een volledig onschuldig stukje code dat door de belangrijkste virusscanners is opgenomen in de signatuurdatabase. Jouw virusscanner reageert vrijwel direct op verdachte bestanden. Dit test je door de volgende opdracht in de juiste volgorde uit te voeren:

a. Rechtsklik op je desktop en kies Nieuw | Nieuw tekstbestand.
b. Op je desktop verschijnt een Notepad-bestandje.
   Hernoem het bestand test.txt en open het lege bestand.

Bekijk de website.

c. Kopieer van de pagina de testcode (in het plaatje hieronder te zien) en plaats dit in het Notepad-bestandje. Sluit het bestand af en sla het op.

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```