Inleiding

Je hebt je aangemeld voor het excellentietraject Ethical Hacking. Het programma is een verdieping op het huidige lesprogramma en is bedoeld voor studenten die extra uitgedaagd willen én kunnen worden op dit thema. Voor dit traject hebben we een beperkt aantal plekken beschikbaar en daarom zal de toelating voor een programma zich richten op 3 pijlers:

- Motivatie in de les (beoordeling van de docent)

- Bereidwilligheid om uren in een extra programma te stoppen (motivatie van de student)

- Toelatingsexamen in de vorm van een netwerk & security challenge

We hebben vanuit verschillende 2e jaars klassen AO, IB en NB via jullie loopbaanbegeleider jullie opgave gekregen om mee te doen. Het vervolg is nu dat jullie deze challenge zo goed en volledig mogelijk maken.

Challenge

Onderstaand vind je de opdracht van deze challenge. Deze opdracht maak je individueel en moet uiterlijk dinsdag 17 april worden ingeleverd. Te laat opgestuurde uitwerkingen worden niet in behandeling genomen. Als je deze opdracht hebt gemaakt kun je de uitwerking (in dit document) mailen naar dhr. Hoogeveen ([e.hoogeveen@rocmn.nl](mailto:e.hoogeveen@rocmn.nl)) en mevr. Speerstra ([b.speerstra@rocmn.nl](mailto:b.speerstra@rocmn.nl)).

Op basis van je antwoorden vindt selectie voor dit traject plaats. Bij twijfel wordt contact gezocht met je loopbaanbegeleider om e.e.a. te bespreken.

1. Doelen

Verken de beveiligingsfuncties gebruikt door organisaties om gegevens veilig te houden.

Deel 1: De dreiging van Cyberattacks verkennen

Deel 2: Confidentiality, Integrity, en Availability (CIA)

Deel 3: Opdracht

1. Achtergrond / Scenario

Dreigingen voortvloeiend uit de cyber-wereld zijn reëel. Deze dreigingen kunnen grote schade aanrichten op onze huidige manier van leven, waarbij ICT een belangrijke rol speelt. Het is belangrijk om inzicht te krijgen in de dreigingen om ze te kunnen bestrijden. De maatschappij heeft mensen nodig die cyber-dreigingen kunnen herkennen om zo cybercriminelen te slim af te zijn.

1. Vereiste middelen

* PC of mobiel apparaat met internettoegang

Deel 1: Verkennen van de dreiging van cyberaanvallen

Cyberattacks staan bovenaan de lijst van dreigingen voor landen over de hele wereld. Wanneer mensen denken aan dreigingen van nationale- of internationale omvang, dan denken de meeste mensen aan fysieke aanvallen met massavernietigingswapens. Het feit is echter dat cyber dreigingen bovenaan de lijst staan van meer dan twintig landen over de hele wereld.

Computers en computernetwerken beïnvloeden de manier waarop we leren, aankopen doen, communiceren, reizen en wonen. Computersystemen controleren bijna elk aspect van ons leven. Een verstoring van deze computersystemen en computernetwerken kan een verwoestend effect hebben op ons huidige, moderne leven. Doelwitten van cyberaanvallen zijn onder andere: De energiesector, systemen voor de behandeling en levering van water, vervoer en financiële systemen zijn allemaal doelwit.

Stap 1: Onderzoek.

In deze stap ga je diverse bedreigingen nader onderzoeken. Beantwoord de volgende vragen zo volledig mogelijk.

1. Klik [hier](https://www.youtube.com/watch?v=WnUuLzXCIEk) om een video te bekijken. Volgens de video: wat is het gevaarlijkste wapen in de wereld en waarom? In hoeverre ben je het hier mee eens (motiveer je antwoord)?

Volgens de video is het gevaarlijkste wapen van de wereld een computer in de handen van een crimineel.

Ik ben het hier niet helemaal mee eens gezien het nucleair arsenaal op de wereld. Welke de kracht hebben om hele regio’s in een oogwenk plat te leggen.Je hebt ook ground to space missiles die dus belangrijke satellieten uit de lucht kunnen schieten wat zeer ontwrichtend kan welken op de infrastructuur en emp bommen die op massale schaal computers en elektronica kunnen doorbranden in een bepaalde regio.

Echter de risico’s zijn wel reëel waardoor het soms zelfs handig is om bepaalde kritieke systemen niet aan te sluiten op het internet om hacks te voorkomen. Denk aan operatie machines in het ziekenhuis bijvoorbeeld.

1. Noteer vijf manieren hoe een cyber-crimineel een computer gebruikt? In hoeverre is het mogelijk dat één van die manieren die je hebt genoteerd je persoonlijk kan raken? In hoeverre ben jij of je familie al eens getroffen door een cyber-aanval?

**5 bedreigingen**

1. Het hacken van een webshop om zo betaalgegevens te bemachtigen.

2. randsomware maken om zo mensen af te kunnen persen.

3. spyware schrijven om zo data van mensen hun machines te vergaren.

4. phising mails versturen om zo mensen geld afhandig te maken.

5. producten verkopen die men nooit levert.

**Mijn risico’s**

Van deze 5 zou ik het makkelijkst getroffen worden door nummer 1. Omdat dit voor het grootste deel buiten mijn macht ligt.

verder kan ik nummer 2 en nummer 3 niet volledig uitsluiten hoewel ik de kans dat dat deze software mij treft niet heel groot acht opdat ik niet zomaar van alles installeer.

En voor nummer 4 en 5 schat ik de kans dat mij dat treft op bijna nul aangezien je met gezond verstand je heel goed kan wapenen tegen deze 2 bedreigingen.

**Bekende gevallen in mijn omgeving**

Persoonlijk ken ik geen mensen die getroffen zijn door een cyber aanval.

1. Noteer tenminste drie recente internationale cyberaanvallen en beschrijf deze zo volledig mogelijk (wat voor soort aanval, wie was het doel, waarom e.d.)

Een vrij recente aanval in 2017 was op Ukraine waar het doel was om het land stevig te verzwakken met het “NotPetya” virus. Dit heeft delen van het land zijn infrastructuur inderdaad plat gelegd. Maar heeft ook computers wereldwijd getroffen. Deze aanval heeft bedrijven miljarden gekost. (Dit had waarschijnlijk een politiek doel om zo Ukraine een les te leren)

In februari 2018 het Duitse nieuws heeft gerapporteerd dat een Russische hackers groepering het online netwerk van het Duitse ministeries van buitenlandse zaken en binnenlands zaken gehackt heeft met een buit van 17 gigabytes aan data Het lek werd pas gevonden nadat de hack al een jaar data aan het verzamelen was. (doel hiervan is waarschijnlijk het verkopen van deze data)

In mei 2017 wordt een grootschalige aanval met randsomeware uitgevoerd welk doel is om geld afhandig te maken van iedereen die geïnfecteerd wordt. De aanval is niet gericht en is bedoeld om geld te eisen van iedereen die ongelukkig genoeg is om geinfecteerd te worden. De aanval maakt gebruik van kwaadaardige software genaamt “WanaCrypt0r 2.0” or WannaCry wat het verspreidingsbereik van deze software aanzienlijk vergroot heeft.

1. Lees [dit artikel](http://www.information-age.com/cybercrime-takes-almost-600bn-toll-global-economy-study-finds-123470890/). Wat zijn de kosten voor de wereldeconomie van cybercriminaleit en welke twee landen zijn leider in cybercrimilaliteit?

**Cyber criminaliteit leiders**

Volgens dit artikel is Rusland leider in cybercrime gevolgd door Noord Korea.

**Totale kosten**

De totale kosten van cybercriminaliteit wereldwijd lopen rond de 600 miljard (0.8% van het wereldwijde BBP)

Deel 2: Confidentiality, integrity, en availability (CIA)

Confidentiality, integrity, en availability zijn de drie fundamentele cyberveiligheid-principes. De elementen zijn de drie meest cruciale onderdelen van de veiligheid. Alle professionals van cyberveiligheid moeten bekend zijn met deze fundamentele principes..

Stap 1: Verken de onderdelen van CIA.

1. Klik [hier](https://www.youtube.com/watch?v=bhLbnOa4wno) om de video te bekijken. Wat is data confidentiality? Waarom is data confidentiality zo belangrijk voor mensen en organisaties?

Met data confidentiality wordt bedoelt dat data die je als organisatie krijgt niet zomaar deelt en je het zo privé mogelijk houdt. Doe je dit niet goed dan kan het enorm het vertrouwen in jou organisatie schaden.

1. Wat is data integrity? Noem drie manieren hoe data integrity wordt beïnvloed.

1. Data integriteit wordt beïnvloed door accuraatheid van de data.

2. Fouten in de data.

3. Het ongewenst aanpassen van de data.

1. Wat is system availability? Wat kan er gebeurden als critische computersystemen niet langer beschikbaar zijn?

**Wat is system availability?**

System availability betekent vrijwel letterlijk wat er staat (de beschikbaarheid van een systeem)

**Wat gebeurt er als kritische computer systemen niet langer beschikbaar zijn?**

Bijvoorbeeld in ziekenhuizen kan het leiden tot uitstel van operaties en bij banken kan het leiden tot uitstel van betalingen en daarmee een hoop schade in euro’s

Deel 3: Opdracht

Het ROC Midden Nederland gebruikt ook vele ICT voorzieningen waaronder Office 365. Microsoft Office 365 is een verzameling van internetdiensten, bedoeld voor bedrijven, thuisgebruik en het onderwijs. Deze internetdiensten worden deels aangeboden als online diensten, deels als applicaties op desktop-pc, tablet en telefoon en als combinatie van beide. De applicaties op desktop / pc is vergelijkbaar met het kantoorpakket Microsoft Office met het verschil dat men via Office 365 altijd de beschikking heeft over de meest recente versie (bron Wikipedia).

**Stap 1: Verken Office 365.**

Maak gebruik van de mogelijkheden die je hebt in Office365 en beantwoord de volgende vragen zo volledig mogelijk.

1. Gebruik je ROC account en verken zo volledig mogelijk de omgeving van Office 365/ROCMN. Noteer hieronder tot welke applicaties je toegang hebt.

Office 365 apps

Agenda

Delve

Exel

Nieuwsfeed

Onedrive

OneNote

Outlook

Personen

Powerpoint

SharePoint

Taken

To-Do

Video

Word

Overige Apps

Blackboard

Drawio

EduArte Student

Office download

Studiegidsen

VIO

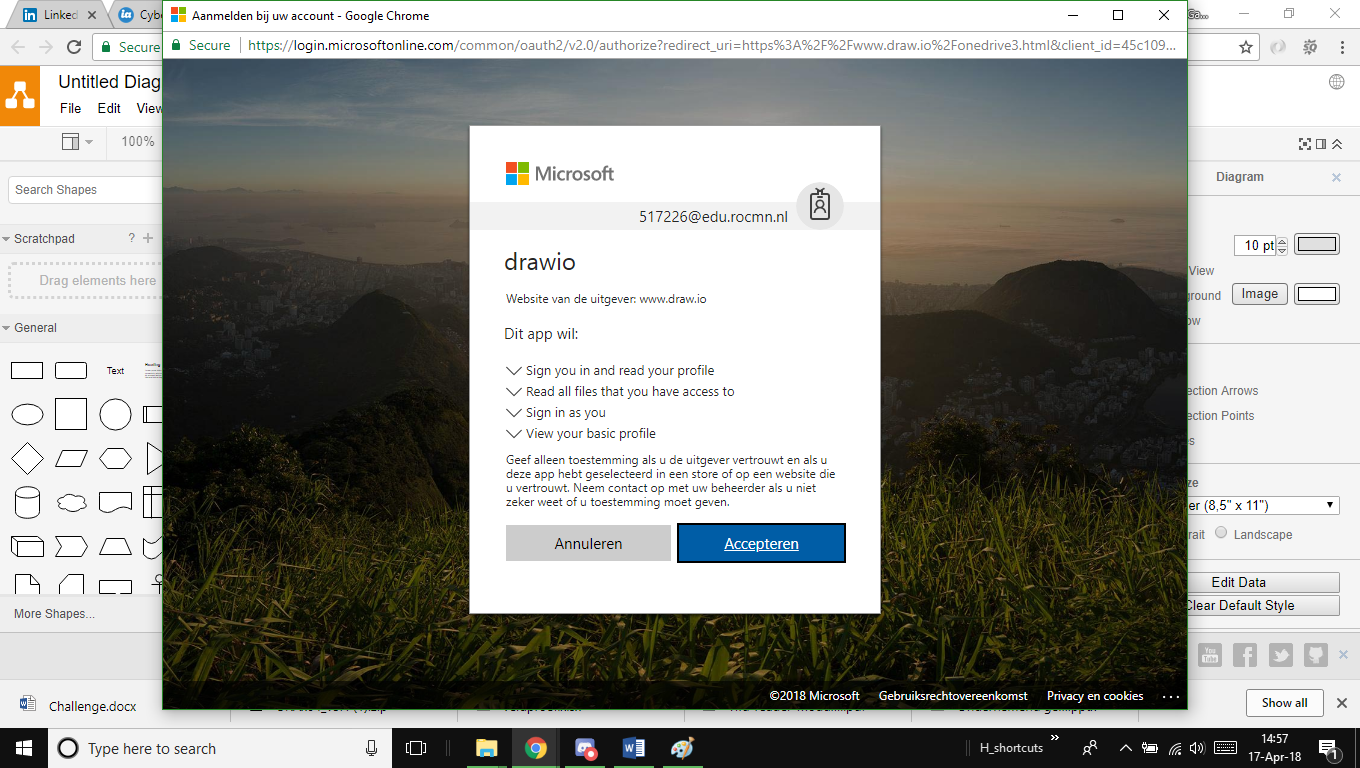
Wachtwoordzelfservice

Webshop

1. Gebruik de diverse applicaties en ga op zoek naar niet beveiligde sites, omgevingen, groepen, etc. en maak een inventarisatie van gegevens. Rapporteer hieronder zo volledig en overzichtelijk mogelijk:

De app drawio vraagt redelijk veel toegangs privileges als je probeert een existent diagram te openen.

Dit maakt het mogelijk voor hun om jou opgeslagen data te verzamelen en voor een niet van tevoren aangegeven doel te gebruiken zoals dit recent met facebook gebeurt is. Hieronder vind je een screenshot van het hele gebeuren



De screenshot is gemaakt op 17 april 2018