

2023

Jono Wink, Thom van der Linden, Reinout Koster en Jari Oud

26-6-2023

Verslag team 6 KPN



# Inhoud

[Inhoud 1](#_Toc138684738)

[Inleiding 2](#_Toc138684739)

[Opdracht 1, oriëntatie voor- en nadelen digitalisering 2](#_Toc138684740)

[1.1 Effecten digitalisering 2](#_Toc138684741)

[1.2 Digitalisatie in huis 2](#_Toc138684742)

[1.3 Digitalisering op school 2](#_Toc138684743)

[1.4 Tot hoever gaat digitalisatie 2](#_Toc138684744)

[1.5 Gevaren van digitalisering 3](#_Toc138684745)

[Poster 3](#_Toc138684746)

[Opdracht 2, cyber crime en cyber security 4](#_Toc138684747)

[2.1 Verschillende Manieren van cybercriminaliteit 4](#_Toc138684748)

[2.2 Hackers 4](#_Toc138684749)

[2.3 Hoe vaak komt cybercrime voor? 4](#_Toc138684750)

[2.4 Encryptie en firewall 4](#_Toc138684751)

[2.5 Hoe is het gesteld met het bewustzijn van de gevaren van cybercriminaliteit? 4](#_Toc138684752)

[2.6 Welke mogelijkheden zijn er voor het voorkomen van cybercriminaliteit? 4](#_Toc138684753)

[2.7 Etische hackers 4](#_Toc138684754)

[Poster 5](#_Toc138684755)

[Opdracht 3A, recente cybercrimes 6](#_Toc138684756)

[3.1 Woonkracht 10 6](#_Toc138684757)

[3.2 Capita 6](#_Toc138684758)

[3.3 Dragos 6](#_Toc138684759)

[3.4 Holland Casino 6](#_Toc138684760)

[3.5 ABB 6](#_Toc138684761)

[Poster 6](#_Toc138684762)

[Opdracht 3B, open source intelligence onderzoek 7](#_Toc138684763)

[8](#_Toc138684764)

[**Beveiligingsadvies Joost Farwerck** 8](#_Toc138684765)

[Phishing test 8](#_Toc138684766)

[Algemene gevaren 8](#_Toc138684767)

[Persoonlijke gevaren 8](#_Toc138684768)

[Advies 8](#_Toc138684769)

[Werkwijze 9](#_Toc138684770)

[Bronnen 9](#_Toc138684771)

# Inleiding

Wij zijn Thom van der Linden, Jono Wink, Reinout Koster en Jari Oud. Voor het derde en laatste O&O project van dit jaar kregen we de opdracht in naam van KPN om onderzoek te doen naar digitalisatie en cybersecurity en daarna een beveiligingsadvies te schrijven voor een zelfgekozen persoon, bedrijf of infrastructureel bouwwerk. Zelf hebben wij gekozen voor de CEO van KPN, Joost Farwerck. In dit verslag lees je onze uitwerking van dit project en nemen we je in detail mee in wat wij allemaal hebben gedaan.

# Opdracht 1, oriëntatie voor- en nadelen digitalisering

## Effecten digitalisering

Als persoon gebruik je veel digitale dingen en dit heeft voordelige en nadelige effecten, een voordelig effect hiervan is bijvoorbeeld dat je altijd met iedereen overal kan communiceren met je telefoon. Een nadelig effect van de digitalisering is bijvoorbeeld dat mensen gameverslaafd raken of dat als het stroom ergens wegvalt dat dan niemand meer iets kan. Iedereen is dus op deze manier helemaal afhankelijk van het internet.

## Digitalisatie in huis

In veel huishoudens worden slimme apparaten gebruikt, dit heten smart home apparaten. Een groot voordeel daarvan is dat je alles met je telefoon of met je stem kan bedienen, dat is een stuk makkelijk dan alles los te bedienen een ander voordeel is dat dingen automatisch gebeuren bijvoorbeeld als je thuis komt gaan de lichten aan. Een nadeel van smart home apparaten is dat niet alle merken van apparaten samen werken met elkaar en als de wifi uitvalt of je wordt gehackt dan is het helemaal niet meer bruikbaar. Een belangrijke factor in de digitalisering van huishouden is het feit dat bijna iedereen tegenwoordig wifi in huis heeft waardoor alle apparaten samen op 1 netwerk kunnen werken.

## Digitalisering op school

Op school maken wij gebruik van magister en outlook voor ons rooster en huiswerk. Een voordeel daarvan is dat als we uitval hebben we dat niet pas op school te horen krijgen. Het nadeel is wel dat docenten altijd nog huiswerk kunnen opgeven. Verder hebben we nog online methodes voor bepaalde vakken, zoals biologie en aardrijkskunde. Voordelen daarvan zijn dat als ik een opgave heb gemaakt ik meteen kan zien of het goed is en dat je je huiswerk ook sneller af hebt, omdat je over het algemeen sneller typt dan schrijft.

## Tot hoever gaat digitalisatie

De digitalisatie gaat tegenwoordig heel erg snel. Je hebt nu zelfs koelkasten en ovens op WI-FI. Gelukkig doen we ook nog dingen zonder iets digitaals zoals naar buiten en op vakantie gaan. Dit komt vooral omdat we dat digitaal nog niet goed na kunnen maken. Ook sporten is ook nog niet helemaal gedigitaliseerd. Dat komt dan weer doordat veel mensen het ook fijn vinden om het buiten te doen.

## Afbeelding met tekst, schermopname, ontwerp Automatisch gegenereerde beschrijving1.5 Gevaren van digitalisering

De gevaren van digitalisering is dat opeens alles online staat, maar dan ook echt alles. Dus als je computer opeens crasht ben je alles kwijt. Je kan ook worden gehackt door bijvoorbeeld op een verkeerde link te klikken, dan kunnen hackers bij allemaal belangrijke dingen zoals je bankrekening en. Hackers kunnen ook hele systemen platleggen voor een bepaalde tijd dat is al een paar keer gebeurt en het heeft die bedrijven veel geld gekost.

## Poster

We hebben alle informatie hierboven verwerkt in een overzichtelijke poster

# Opdracht 2, cyber crime en cyber security

## 2.1 Verschillende Manieren van cybercriminaliteit

* Phishing is een manier van cybercirminaliteit. Via e-mails, berichten en websites wordt er vaak een link opengezet waar je op MOET klikken. Als je op de link klikt hebben de hackers je persoonlijke informatie of financiële gegevens.
* Ransomware. Ransomware werkt zo dat het slachtoffers computer of laptop versleuteld wordt, waardoor ze niks meer op de computer kunnen doen. De hackers eisen vaak geld via bitcoin.
* DDoS-aanval. Via een DDoS-aanval wordt een website of netwerk overbelast met een enorme hoeveelheid ''verkeer'' om het systeem plat te leggen.
* Cyberstalking: Het online bedreigen of intimideren van een persoon.
* Cyberterrorisme: Het gebruik van digitale technologieën door terroristische groeperingen om chaos en paniek te creëren

## 2.2 Hackers

Hackers zijn mensen die in systemen van bedrijven of personen willen komen en hebben slechte bedoelingen deze soort hackers worden ook wel black hats genoemd deze mensen zijn de grootste oorzaak bij cybercriminaliteit

## 2.3 Hoe vaak komt cybercrime voor?

13 procent van Nederland heeft wel eens last gehad van cybercrime en om de 53 seconden wordt er een laptop gestolen. Er zijn ook veel gratis apps op je telefoon die toestemming hebben om al je gegevens te bekijken zonder dat jij het doorhebt. Deze gegevens worden doorverkocht en er wordt vaak een online profiel van je gemaakt waarmee adverteerders jou kunnen bestuderen en je andere advertenties kunnen geven dan iemand anders.

## 2.4 Encryptie en firewall

Dat zijn twee manieren om jezelf of je bedrijf te beschermen tegen cybercriminaliteit. Hoe dit precies werkt in de computer is erg ingewikkeld, maar het komt neer op dat je je computer of bedrijfssysteem beschermt met een bepaalde versleuteling of beveiliging waardoor het hackers meer moeite kost om in het systeem te komen. Ze zullen het daarom niet proberen of het lukt ze niet.

## 2.5 Hoe is het gesteld met het bewustzijn van de gevaren van cybercriminaliteit?

Veel mensen weten niet hoe veel informatie de apps op bijvoorbeeld je telefoon over jou kunnen krijgen. Ook kunnen hackers makkelijk doormiddel van phishing met een echt uitziende link veel informatie krijgen.

## 2.6 Welke mogelijkheden zijn er voor het voorkomen van cybercriminaliteit?

Cybercriminaliteit is te voorkomen doormiddel van een vpn (virtual private network) bijvoorbeeld nord vpn waarbij de informatie die je device uitstuurt in een laag van encryptie komt en waardoor niemand jou informatie kan zien. Dit werkt doordat nord vpn een veilige verbinding creëert waar hackers niet bij kunnen komen.

## 2.7 Etische hackers

Etische hackers zijn de soort hackers die hacken met goede bedoelingen doen. Zij hacken de systemen van bedrijven om fouten te vinden en dan kan het bedrijf ze daarna verbeteren zij hacken dus met goede bedoelingen.

## Poster

Alle informatie die we u hebben gegeven hebben we verwerkt in een poster. Die kan u hieronder zien. 

# 

# Opdracht 3A, recente cybercrimes

## 3.1 Woonkracht 10

Woonkracht10, een woningcorporatie, werd slachtoffer van een ransomware-aanval. Ze waren gedwongen om geld te betalen om te voorkomen dat de aanvallers gestolen gegevens zouden publiceren.

## 3.2 Capita

Capita, een Britse dienstverlener, werd ook getroffen door een ransomware-aanval. Ze verwachten dat de kosten van deze aanval kunnen oplopen tot 23 miljoen euro.

## 3.3 Dragos

Het cybersecuritybedrijf Dragos meldde een eigen cybersecurity-incident en afpersingspoging. Dit betekent dat ze zelf het doelwit waren van een aanval waarbij de aanvallers hen probeerden te dwingen tot betaling.

Afbeelding met tekst, Lettertype, schermopname, document

Automatisch gegenereerde beschrijving

## 3.4 Holland Casino

Holland Casino heeft te maken gehad met een DDoS-aanval, waarbij het online platform tijdelijk werd platgelegd. Een DDoS-aanval houdt in dat een grote hoeveelheid verkeer naar een website wordt gestuurd om deze te overbelasten en onbruikbaar te maken. In dit geval wordt vermoed dat Playtech, een bedrijf dat online gamingsoftware levert, het doelwit van de aanval was.

## 3.5 ABB

Het multinationale technologiebedrijf ABB is ook getroffen door een ransomware-aanval genaamd Black Basta. Dit betekent dat de aanvallers de systemen van ABB hebben geïnfecteerd en losgeld hebben geëist.

## Poster

Ook van deze informatie hebben wij een poster gemaakt die hiernaast te vinden is.

# Opdracht 3B, open source intelligence onderzoek

Persona CEO KPN

Naam: Joost Farwerck

Geboorte: Hilversum 1965

Nationaliteit: Nederlands

Zit in de managmement van KPN sinds: 2013

Hij heeft ook allemaal andere dingen gedaan bij KPN zoals: consumer residentual buisness, salesmanager, wholesale operations

Kwam bij KPN in 1994

Verdient per jaar 875 duizend euro met bonussen van een paar miljoen

Zit bij de: FME, NL-cybersecurity, lid van Raad van Toezicht Stichting Lezen & Schrijven, lid van de Raad van Toezicht Nieuwe Kerk Amsterdam.

Zat bij de: ibasis, vno, nwc

Woont in Den Haag

Vader van drie en getrouwd

Hij doet aan rennen fietsen en tennis

Hij houdt van literatuur

Hij studeerde rechten in Amsterdam

Joost heeft geen andere sociale media dan Linkedin

[joost.farwerck@KPN.com](mailto:joost.farwerck@kpn.com)

Afbeelding met tekst, schermopname, Lettertype, software

Automatisch gegenereerde beschrijving[j.farwerck@planet.nl](mailto:j.farwerck@planet.nl)

Phising test: Wij hebben een Phising mail gestuurd naar Joost Farwerck waarop wij een reactie kregen van een security team van KPN. In de mail stond dat Joost de phising mail naar hun door had gestuurd en dat hij er dus niet in was getrapt.

Afbeelding met tekst, schermopname, Lettertype

Automatisch gegenereerde beschrijvingBronnen: ContactOut en linkedin

## Afbeelding met Menselijk gezicht, persoon, kleding, Formele kleding Automatisch gegenereerde beschrijving

## **Beveiligingsadvies Joost Farwerck**

**Wij hebben afgelopen tijd onderzoek gedaan naar de CEO van KPN, Joost Farwerck. Wij hebben een persona van hem opgesteld en gekeken naar zijn digitale beveiliging. Vanuit deze informatie hebben wij een beveiligingsadvies opgesteld om de digitale beveiliging van Joost Farwerck te verbeteren.**

## Phishing test

Wij hebben zelf een mail gestuurd naar Joost Farwerck waarin wij een phishing link geplakt hadden. Op deze mail kregen wij een reactie van het KPN-CERT (computer emergency response team) dat Joost in plaats van op de link te klikken de mail naar zijn beveiligingsteam gestuurd heeft. Hierdoor weten wij dat Joost goed beveiligd is tegen phishing.

## Algemene gevaren

Cybersecurity is bij iedereen van belang. Veel mensen klikken op phishing mails waardoor criminelen gelijk veel informatie van ze hebben. Mensen hebben ook vaak te simpele wachtwoorden die met een simpel programma zo worden gehackt. Omdat meneer Farwerck CEO is van KPN willen we hem ook adviseren voor deze gevaren. Hij is zelf goed beschermt tegen deze algemene gevaren, maar hij moet er ook op letten dat al zijn werknemers zich goed bewust zijn van de gevaren. Wanneer een crimineel in de computer van iemand in KPN kan komen, zitten ze gelijk in het systeem van KPN en daardoor kunnen ze ook makkelijker bij andere computers komen zoals die van de CEO van het bedrijf.

## Persoonlijke gevaren

Wij hebben met een simpel onderzoek Heel veel informatie gevonden over Joost Farwerck waarvan wij dachten dat het beter was als het niet online stond, bijvoorbeeld: zijn e-mailadres was makkelijk online te vinden (zowel zijn business mail als persoonlijke mail), ook was het zo dat wij door zijn mail in te voeren in de ´´have i been pwned´´ website erachter zijn gekomen dat er maar liefst 7 data leaks zijn geweest van Joost zijn privéinformatie, waaronder e-mailadressen en wachtwoorden.

## Advies

Ons beveiligingsadvies voor Joost Farwerck is om goed op te letten wat er allemaal over hem op het internet te vinden is. Wij konden namelijk met een simpele ´google search´ veel informatie over hem vinden waaronder zelfs zijn privé mail en werk mail. Dit is best gevaarlijk want iedereen kan met deze mail Joost een phishing mail sturen.  Een data lek heeft ook nog andere gevaren zoals: Identiteitsfraude door bijvoorbeeld een wachtwoord, oplichting als criminelen belangrijke informatie over je hebben en inbraak als je adres bekend is. Ons tweede advies is om goed op te letten op de beveiliging van zijn medewerkers, want als zijn medewerkers gehackt worden kunnen ze via het systeem van KPN makkelijker in de computer van Joost komen. Ook hebben wij Joost zijn mail op de ´have i been pwned´ website ingevoerd en zijn er hiermee achter gekomen dat Joost zijn data op maar liefst 7 verschillende plekken gelekt is dit houdt in dat mensen op het internet dingen zoals Joost zijn wachtwoorden van bepaalde sites kunnen achterhalen. Dus als Joost voor meerdere sites hetzelfde wachtwoord heeft dan kan een hacker daar allemaal heel makkelijk bij. Wij adviseren hem dus dat hij goed in de gaten moet houden welke data van hem gelekt wordt en zorgen dat als het belangrijke informatie is hij ervoor zorgt dat hackers daar niks mee kunnen door bijvoorbeeld wachtwoorden te veranderen.

# Werkwijze

Wij hebben de opdrachten veel samen gemaakt en dan binnen de opdracht een taakverdeling gemaakt per en duidelijk afgesproken wanneer het af moet zodat we daarna weer door konden. We hebben ook een aantal dingen helemaal samen gemaakt zodat we goed konden brainstormen en tot het best idee komen om daarna uit te werken. We hebben deze manier van werken allemaal heel prettig ervaren en het project is dan ook heel goed gegaan.

# Bronnen

ContactOut

Linkedin

KPN

Canva

have I been pwned