



OPEN SOURCE INTELLIGENCE (OSINT) & PHISHING

Opdracht Week 1

INFORMATIE

Dit document is geschreven door Tom Stuurman & Abe Bruinsma

Opdracht 1, Oriëntatie:

Het bedrijf dat onderzocht is heet Akzonobel. Akzonobel is een Nederlandse multinational die gespecialiseerd is in het maken en verkopen van verf en coatings. Het bedrijf levert toonaangevende merken zoals Flexa, Sikkens, International en Interpon aan klanten over de hele wereld. De primaire bedrijfsprocessen van Akzonobel is op de delen in 3 delen: 1. De productie van verf en coatings in verschillende landen. 2. Akzonobel verkoopt wereldwijd zijn producten. 3. Ze leveren klantenservice en technische ondersteuning voor hun producten en diensten.

Opdracht 2, bedrijfsflags verzamelen:

We begonnen met een pagina maken in OneNode. Hierna gingen we gelijk door met het opzoeken naar de flags. Onze werkwijze ging als volgt: We gingen zoeken naar wat we konden vinden over het bedrijf en als we wat hadden gevonden gingen we kijken of het een flag was. Hieronder staat een lijst met dingen die we hebben gevonden doormiddel van OSINT.

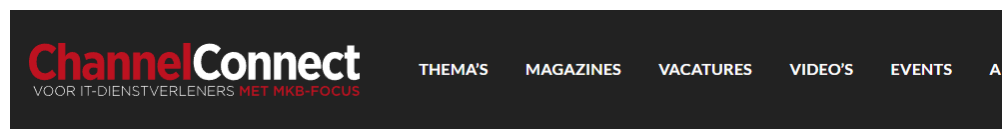
Omdat Akzonobel een groot bedrijf is hebben we gezocht naar de locaties in Nederland. We kwamen er al snel achter dat de hoofdlocatie in Amsterdam is. Hierdoor konden we meer gespecificeerde zoeken.

1. Wie verzorgt de ICT-diensten? Is het in-house of outsource:

Wat: De ICT is outbound door het bedrijf Orange.

Waar: Dit document is gevonden door een simpele zoekterm ICT Akzonobel.

<https://www.channelconnect.nl/security-en-privacy/orange-business-services-richt-soc-in-voor-akzonobel/>



SECURITY NIEUWS

Orange Business Services richt SOC in voor Akzo Nobel

8 april 2020, 11:41 Door Edwin Feldmann

Akzo Nobel heeft de samenwerking met Orange Business Services verlengd, onder meer voor het verbeteren van de cyberbeveiliging.

Orange Business Services ondersteunt Akzo Nobel bij het centraliseren van IT/OT-netwerkactiviteiten. Daarnaast richt Orange een CyberSOC op om de end-to-end beveiliging te controleren voor zowel IT als OT.

Het bedrijfsonderdeel Orange Cyberdefense zal voor Akzo Nobel forensic security, beveiligings- en risicoanalyse samenbrengen. Orange stelt ook aanvullende beveiligingsprocessen op voor de netwerkinfrastructuur van het bedrijf, onder andere voor gebruikers van roaming en voor derde partijen. Orange zal de diensten en technologieën van meerdere netwerkleveranciers beheren met behulp van een MSI-model.

<https://www.orange-business.com/en/press/akzonobel-partners-orange-business-services-drive-digital-transformation-secure-end-end>

**Business**

Business needs Our solutions About us

 > Press Releases

AkzoNobel partners with Orange Business to drive digital transformation with secure end-to-end global connectivity services

April 07, 2020 | Paris, France



- Solution includes software-defined networking and security services, including a CyberSOC
- IT/OT network convergence driven by productivity and operational security requirements

AkzoNobel has expanded its agreement with [Orange Business](#) to transform its global network and security infrastructure, converge information technology/operational technology (IT/OT) and enhance security. The partnership will enable AkzoNobel to scale up its innovation budget and drive digital transformation.

Orange is providing a range of services, including [software-defined WAN](#) and LAN, [multisourcing service integration \(MSI\)](#), [security](#) and [consulting](#) services for AkzoNobel's global connectivity transformation. Orange will also support AkzoNobel in centralizing its IT/OT network operations, connecting and managing its entire footprint from factory to store, across all regions.


Risicoanalyse: De eventuele aanvaller weet nu dat ze de ICT niet zelf doen maar dat Orange dat doet.


Oplossing: Er is niet perse een oplossing. Orange heeft zelf gepubliceerd dat ze samen in zee gaan met Akzonobel.

2. Welke e-mail client:


Wat: Ze maken gebruik van @akzonobel.com.

Waar: Via Hunter.io hebben we het bedrijfsnaam Akzonobel ingevoerd.

 Log in [Sign up](#)

 **akzonobel.com**
All the email addresses found for akzonobel.com ©

1,357 results for your search Email pattern: `{first}.{last}@akzonobel.com`

i **a@akzonobel.com**  5 sources


<http://sanctuarycoveboatshow.com.au> Dec 13, 2023

<http://sanctuarycoveboatshow.com.au/exhibit> Dec 13, 2023

<http://sanctuarycoveboatshow.com.au/partners> Dec 13, 2023

<http://sanctuarycoveboatshow.com.au/sanctuary-cove> Dec 13, 2023

<http://sanctuarycoveboatshow.com.au/show> Dec 13, 2023

e **g@akzonobel.com**  4 sources

<http://b2b8.com/article/314.html> Dec 15, 2023

<http://b2b8.com/article/list-article-10684.html> Dec 15, 2023

Bronvermelding: <https://hunter.io/try/search/akzonobel.com?locale=en>

Risicoanalyse: Wat mogelijk is, is een phishing mail sturen met een domain naam die er heel erg op lijkt. Ook kunnen ze je email spoofen. De hacker maakt een mail adres aan met bijna dezelfde naam.

Oplossing: De ITer daar moet een cursus geven aan de medewerkers dat je niet zo maar op linkjes moet klikken als het mail adres bekend voor komt. Het kan namelijk zijn dat de mail adres word gespoofed.

3. Wat voor computers worden er gebruikt:

Wat: We hebben gezien dat ze gebruik maken van HP Pavilion laptops. Ook hebben ze geen vaste werkplekken waardoor we kunnen stellen dat ze of BYOD gebruiken of ze een laptop van de zaak krijgen. Aangezien we hebben gelezen dat ze HP een leverancier van Akzonobel is, denken wij dat ze een werklaptop krijgen.

Waar: Deze flag is gevonden bij de google images. Hier zagen wij dat de medewerkers gebruik maken van de HP laptops.



<https://www.frankhanswijk.nl/portfolio/architectuur-stedenbouw/groupa-akzonobel-center-and-ar.html#&gid=1&pid=20>



<https://www.frankhanswijk.nl/portfolio/architectuur-stedenbouw/groupa-akzonobel-center-and-ar.html#&gid=1&pid=22>

Op deze foto is goed te zien dat ze gebruik maken van flexplekken omdat ze een laptop koppelen aan een monitor.



DCA HEEFT EEN DATACENTER OP BEDRIJVENCOMPLEX KLEEFSE WAARD IN ARNHEM

behoefte aan eigen datacentercapaciteit in Arnhem. Het concern koos voor een internationale aanpak en ging in de jaren erna onder meer in zee met externe leveranciers als Atos, Orange en HP/EDS. Omdat het belang van het twindatacenter afnam werd tevens besloten te stoppen met het aanbieden van commerciële

<https://www.computable.nl/2016/04/22/pareltjes-data-center-arnhem/#:~:text=DCA%20heeft%20%C3%A9%C3%A9n%20datacenter%20op,jaren%20colocatiediens%20aan%20andere%20bedrijven.>

Risicoanalyse: Omdat we weten dat HP de leverancier is kan er worden gekeken naar de HP laptop of er ook lekken zijn.

Oplossing: De afbeeldingen waren te vinden bij de fotograaf die fotos heeft gemaakt van het pand. De fotograaf moet beter nadenken wat hij op de webpagina zet.

4. Heeft het bedrijf datacentra in eigen beheer, huren ze ruimte in een datacenter, huren ze apparatuur, of gebruiken ze een cloud platform?:

Wat: Akzo Nobel selecteert Atos OneCloud voor beheer publieke en private cloud. Ze gaan naar de cloud omgeving.

Waar: Ik heb deze pagina gevonden door te googelen naar: Datacenter Akzonobel.

AkzoNobel selecteert Atos OneCloud voor beheer publieke en private cloud

Amstelveen, 9 december 2021 – Atos is door AkzoNobel geselecteerd voor het beheer van zijn private en publieke cloud-omgeving, als onderdeel van AkzoNobel's cloud migratie strategie. Hiermee beoogt AkzoNobel de complexiteit van zijn processen te verlagen en zijn business flexibiliteit te verhogen. Deze overeenkomst omvat de vernieuwing van de bestaande private cloud omgeving die al door Atos wordt beheerd en een uitbreiding in de vorm van een publieke cloud-omgeving.

https://atos.net/nl/2021/persberichten_2021_12_13/akzonobel-selecteert-atos-onecloud-voor-beheer-publieke-en-private-cloud

Risicoanalyse: Als hackers willen weten wie de data beheer weten ze nu dat ATOS het beheerd.

Oplossing: Het bedrijf ATOS heeft zelf dit document gepubliceerd. Dus ik denk dat ze wel weten wat ze aan het doen zijn.

5. Ontwikkelt het bedrijf haar eigen tooling/software? Zo nee, aan welke partij wordt dit uitbesteed?

Wat: In een podcast vertellen dat ze gebruik maken van een tool via Azure die ze aan klanten uitgeven.

Waar: Deze informatie komt van een podcast. Ze hebben Martijn Steggink geïnterviewd. Martijn is Color Marketing Digital Tools Manager bij AkzoNobel.

<https://cloudrepublic.nl/26-op-bezoek-bij-akzonobel/>

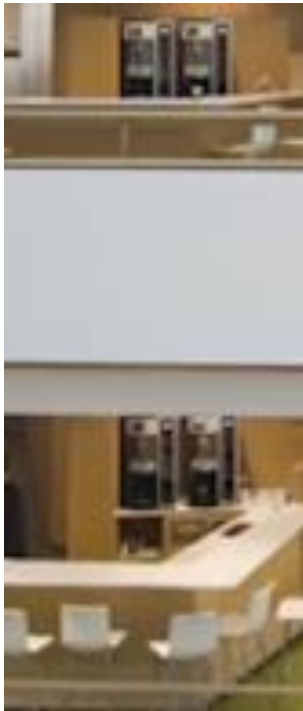
Risicoanalyse: Als ze vertellen waarvan ze gebruik maken weten hackers dat ook. Het kan dat ze verder gaan zoeken naar wat voor tools het zijn via Azure. Zo kunnen ze erachter komen wat de zwakke punten zijn in het systeem.

Oplossing: Niet vertellen aan derde partijen wat voor software er gebruikt wordt in je bedrijf.

6. Welk bedrijf verzorgt de on-site snoep/drankautomaten:

Wat: Ze hebben op hun hoofdkantoor in Amsterdam een Douwe Egberts koffie machine staan.

Waar: Op de foto's is te zien dat ze deze machines gebruiken. Deze fotos staan bij google images als je de locatie opzoekt.



Deze is ook van dezelfde fotograaf:



<https://www.frankhanswijk.nl/portfolio/architectuur-stedenbouw/groupa-akzonobel-center-and-ar.html#&gid=1&pid=11>

Risicoanalyse: Het kan dat een hacker een Social Engineering poging doet voor onderhoud op de machines, maar hij eigenlijk opzoek gaat naar ethernetpoorten.

Oplossing: Goed checken of er echt een monteur langskomt voor onderhoud. Als dit niet zo is moet je hem weg sturen.

7. Is er een on-site draadloos netwerk? +1 voor het (E)SSID:

Wat: Er is een draadloos netwerk in het gebouw. Er word namelijk gebruik gemaakt van access points.

Waar: Hier zijn ook een aantal fotos van op google images



<https://www.google.com/maps/place/AkzoNobel+Center/@52.3401536,4.8776947,3a,75y,90t/data=!3m8!1e2!3m6!1sAF1QipMiS-sevduxw-QRBF5bB909hMFZmf318KTVp5uM!2e10!3e12!6shttps:%2F%2Ffh5.googleusercontent.com%2Fp%2FAF1QipMiS-sevduxw-QRBF5bB909hMFZmf318KTVp5uM%3Dw203-h152-k-no!7i4032!8i3024!4m19!1m9!3m8!1s0x47c60a1b5cce3bb:0x4c182cd3e6c4ff2d!2sChristian+Neefesstraat,+Amsterdam!3b1!8m2!3d52.3399122!4d4.8777842!10e5!16s%2Fg%2F11c52x55bt!3m8!1s0x47c60a041133379b:0xff5b56ba99fa2c1b!8m2!3d52.3401536!4d4.8776947!10e5!14m1!1BCglgAQ!16s%2Fg%2F1tk6zpqz?authuser=0&entry=ttu>



<https://www.google.com/maps/place/AkzoNobel+Center/@52.3401536,4.8776947,3a,75y,90t/data=!3m8!1e2!3m6!1sAF1QipPB16F41IVWDLq3krgrAeOg48r178hDVAgLNCp6!2e10!3e12!6shttps:%2F%2Ffh5.googleusercontent.com%2Fp%2FAF1QipPB16F41IVWDLq3krgrAeOg48r178hDVAgLNCp6%3Dw203-h270-k-no!7i3024!8i4032!4m19!1m9!3m8!1s0x47c60a1b5cce3bb:0x4c182cd3e6c4ff2d!2sChristian+Neefesstraat,+Amsterdam!3b1!8m2!3d52.3399122!4d4.8777842!10e5!16s%2Fg%2F11c52x55bt!3m8!1s0x47c60a041133379b:0xff5b56ba99fa2c1b!8m2!3d52.3401536!4d4.8776947!10e5!14m1!1BCglgAQ!16s%2Fg%2F1tk6zpqz?authuser=0&entry=ttu>

Deze foto is te vinden op de website van dezelfde fotograaf.



<https://www.frankhanswijk.nl/portfolio/architectuur-stedenbouw/groupa-akzonobel-center-and-ar.html#&gid=1&pid=16>



<https://www.frankhanswijk.nl/portfolio/architectuur-stedenbouw/groupa-akzonobel-center-and-ar.html#&gid=1&pid=22>

Risicoanalyse: Het kan zijn dat er een verkeerde configuratie is in een AP. Hierdoor kan een hacker makkelijk naar binnen.

Oplossing: De APs moeten een goede en beveiligde configuratie hebben.

Opdracht 3, Flag Medewerker

Als person of interest hebben we Dick Sluimers uitgekozen omdat hij meerdere rollen binnen Akzonobel vertegenwoordigd.

1. **Hoe lang werkt de werknemer al bij het bedrijf?**

HUIDIGE FUNCTIES DICK SLUIMERS

2019 - heden Commissaris (voorzitter), NIBC

2018 - heden Commissaris (vice-voorzitter), Euronext

2015 - heden Commissaris, AkzoNobel

2016 - heden Staatsraad in buitengewone dienst, Raad van State

2016 - heden Lid board of directors, FWD Group Limited, Hong Kong

LOOPBAAN DICK SLUIMERS

2015 - 2019 Commissaris (vice-voorzitter), NIBC

2005 - 2019 Commissaris, Atradius

2016 - 2018 Commissaris, Euronext

2011 - 2017 Lid of Board Trustees, IFRS Foundation, London

2008 - 2015 Voorzitter raad van bestuur, APG groep

2007 - 2008 Voorzitter directieraad, ABP

2003 - 2007 Directeur Financiën, ABP

1991 - 2003 Plaatsvervangend thesaurier-generaal en directeur-generaal van de Rijksbegroting, Ministerie van Financiën

1988 - 1991 Diverse functies, Ministerie van Volksgezondheid, Welzijn en Sport

1982 - 1988 Diverse functies, Ministerie van Sociale Zaken en Werkgelegenheid

1979 - 1982 Diverse functies, Ministerie van Financiën

Lid raad van toezicht, Netspar

OPLEIDING DICK SLUIMERS

Economie, Erasmus Universiteit Rotterdam

Politieke Wetenschappen, Universiteit van Amsterdam



OVERIGE VERMELDINGEN

NIBC

- Voorzitter Audit Committee

AkzoNobel

- Voorzitter Remuneration Committee
- Lid Audit Committee

Atradius

- Lid Board of Directors Atradius CYC (Madrid)
- Lid Audit Committee

Euronext NV

- Voorzitter Nomination Committee
- Voorzitter Raad van Commissarissen Euronext Amsterdam NV

FWD Group Limited

- Lid Audit Committee

Overige nevenfuncties

- Lid Bestuur Concertgebouwfonds (Amsterdam)
- Lid Curatorium Rijksacademie voor Financiën en Economie (Den Haag)
- Lid Raad van Toezicht Erasmus Trustfonds (Rotterdam)
- Lid Bestuur van de Stichting voor Oeconomische Politiek (Amsterdam)
- Lid Bestuur Dresselhuys Fonds (Den Haag)
- Adviseur Quore Capital (Amsterdam)
- Adviseur Hemingway Corporate Finance (Amsterdam)
- Adviseur Hakluyt & Company (Londen)
- Lid Adviesraad Spencer Stuart (Amsterdam)



TRIVIA

Dick Sluimers woont met zijn partner Filippien in Wassenaar. Hij is vader van drie kinderen. Zijn hobby's zijn sport , lezen en reizen.

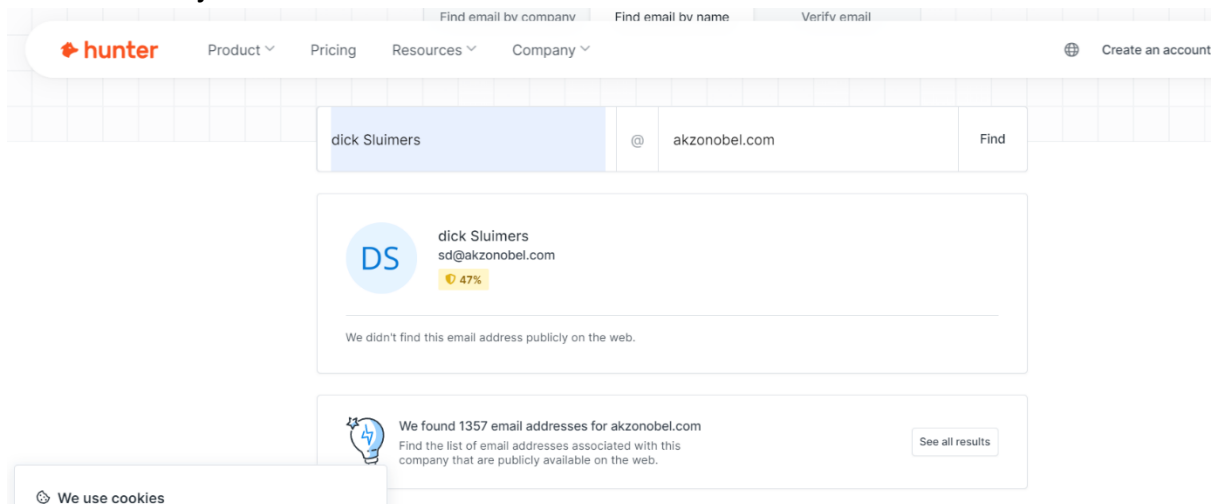
[Dick Sluimers - NIBC & AkzoNobel - Commissaris \(managementscope.nl\)](#)

De gehele loopbaan inclusief extra informatie is te vinden op de bovenstaande site. Dit verteld ons waar hij heeft gewerkt, wat zijn potentiële contacten zijn, en in welke groepen hij te vinden is.

Risico's:

Het gevaar van deze informatie hoog. Een kwaadwillend persoon, zou op basis van deze informatie een phishing mail kunnen schrijven en zich voordoen als een oude collega die hem bijvoorbeeld uitnodigt om een lezing bij te wonen.

2. Wat zijn het interne telefoonnummer en e-mailadres van de medewerker?



The screenshot shows the Hunter.io search interface. At the top, there are navigation links: 'Find email by company', 'Find email by name', and 'Verify email'. The main search bar contains 'dick Sluimers' and '@ akzonobel.com'. Below the search bar, the results show a profile for 'dick Sluimers' with email 'sd@akzonobel.com' and a 47% confidence score. Below the profile, it states 'We found 1357 email addresses for akzonobel.com' and provides a link to 'See all results'.

Op basis van de al gevonden bedrijfsstandaard van Akzonobel samen met de naam, kwamen we via hunter.io op het emailadres van Dick.

risico's:

Doordat we nu het emailadres in handen hebben, zou een bad actor hem een rechtstreekse phishingmail kunnen sturen.

Oplossing:

awarenesstraining, e-mailbeveiliging, beperkte toegang tot contactgegevens.

3. Zijn er belangrijke ontwikkelingen in het bedrijf gaande die belangrijk zijn voor de medewerker?

Mrs. Jolanda Poots-Bijl and Mr. Dick Sluimers were both reappointed as member of the Supervisory Board.

[Ben Noteboom appointed as member of AkzoNobel's Supervisory Board | AkzoNobel](#)

Dick zijn termijn is net weer doorgezet in dezelfde positie.

Risico: Het feit dat hij herbenoemd is al lid van de raad van toezicht kan van belang zijn voor inverteerders. Doordat hij al lang bekend is met het bedrijf en waarschijnlijk er goed in verwoven is, kan het zijn dat insiders of concurrenten hierop in kunnen gaan spelen met bijvoorbeeld de aandelen in het bedrijf.

Oplossing:

Om dit zoveel mogelijk voor de buitenwereld afgeschermd te houden, zou het verstandig zijn om deze informatie alleen zichtbaar te maken voor de mensen met legitiem belang. Dit zou kunnen met een account op de site, zodat er bijgehouden kan worden wie welke informatie heeft bekeken.

Opdracht 4, Pretext

We hebben gezien dat ze koffiemachines gebruiken van Douwe Egberts. Met die informatie wordt de prefix geschreven.

- Wie & Wie:

Wij zijn medewerkers van Douwe Egberts. Wij (Tom en Abe) komen voor onderhoud aan de koffiemachine. Wij komen in contact met de servicebalie medewerker die je ziet als je het gebouw binnen loopt. We gaan de balie medewerker aanspreken.

- Waarom:

Wij hebben contact gezocht omdat er om de zoveel tijd een standaard check plaats vindt op de machines. Wij als DE medewerkers willen liever voorkomen dan genezen. We willen contact opnemen met de servicebalie medewerker. Deze kan ons dan laten zien waar de machines staan

- Wat:

Omdat we met zen 2en zijn kan 1 iemand bij de machine staan en de andere een ethernet poort opzoeken waar we onze raspberry kunnen inpluggen. Op de raspberry staat een scan tool zodat we de netwerk gegevens kunnen krijgen. In het beste geval kunnen we een backdoor maken waarmee we verbinding kunnen maken. Uiteindelijk hopen wij met de informatie belangrijke gegevens te kunnen onderscheppen en die tegen hun gebruiken, zoals wachtwoorden of interne documenten.

- Vraag & antwoord

Er wordt gevraagd aan de balie medewerker waar alle machines staan. Dit doen we zodat we onze kansen uitbreiden op het vinden van een ethernet poort.

We vragen of we speciale toegangsrechten of badges nodig zijn om toegang te krijgen tot de machine.

- Context:

Wij gaan eerst met de balie medewerker bellen om te vragen of er tijd is voor de onderhoud. We spreken vervolgens een datum af om langs te komen.

- Succes kans:

Ik denk dat deze prefix wel te geloven is. Als wij aankomen in echte werkkleding van DE is het wel mogelijk om binnen te komen. Ik denk dat het vooral goed is om van te voren te bellen voor een afspraak. Dan staat het ook in de agenda van de balie medewerker. Waar we wel door de mand kunnen vallen is als ze gaan valideren of wij wel echt van DE zijn. Misschien gaat de balie medewerker bellen naar de om te vragen of ze monteurs hebben langs gestuurd. Het kan ook zijn dat er de hele tijd iemand met ons meeloopt, maar over het algemeen denk ik dat dit een succesvolle poging is.

Opdracht 4, Pretext 2.0

In het artikel op managementscope die we eerder lieten zien, stond dat Dick politieke wetenschappen gestudeerd heeft aan de universiteit van Amsterdam. Door onderzoek te doen naar de universiteit, kwamen we volgend artikel tegen. ["The topics are very up-to-date and have made me understand more about the world around me." - Bachelor Political Science - Universiteit van](#)

[Amsterdam \(uva.nl\)](https://uva.nl)

Hieruit ontstond onderstaand idee

- Wie & Wie:
Alice barlaam, een vertegenwoordiger van de studie politicologie aan de universiteit van Amsterdam
- Waarom:
Onder de indruk van zijn prestaties en loopbaan.
- Wat:
- Uitnodiging op als gastspreker op te treden op de universiteit van Amsterdam tijdens een evenement
- Vraag & antwoord
We willen informeren of de heer Sluimers interesse heeft om als gast spreker op ons evenement op te treden en of de voorgestelde datum in zijn schema past.
- Context:
Om de heer Sluimers te helpen bij het overwegen van deze uitnodiging, hebben we een pdf bijgevoegd met uitgebreide informatie over het evenement. In deze pdf zal dan een payload zitten.
- Succeskans:
Gezien de invloedrijke achtergrond van Dick en vanuit de interviews en videos die hij gedaan heeft, geloven we dat deze pretext een goede kans van slage heeft.

Opdracht 5, Phishing mail

Subject: Invitation to Speak at UvA Political Science Event

Dear Mr. Dick Sluimers,

My name is Alice Barlaam, a second-year Political Science Bachelor student at the University of Amsterdam (UvA), and I am writing to you on behalf of the UvA Political Science community.

Firstly, I want to express my admiration for your distinguished career and the impactful roles you have held, not only as a Commissaris at AkzoNobel but across various significant positions. Your journey, spanning both public and private sectors, serves as an inspiration to students like me who are passionate about understanding political, economic, and societal dynamics.

As a student who appreciates the intersectionality of political, economic, and societal dynamics, I believe your insights would greatly benefit our community. Therefore, I am extending an invitation for you to join us as a guest speaker at one of our upcoming events. Your reflections on your career journey, the challenges you've navigated, and the lessons learned would undoubtedly resonate with our diverse and ambitious student body.

To assist you in considering this invitation, I have attached a PDF containing detailed information about the event, along with a schedule for the day.

If you find this opportunity aligning with your schedule and interests, we would be honored to coordinate further details. Please feel free to reach out to me directly at edss@uva.nl.

I look forward to the possibility of welcoming you to the University of Amsterdam.

Warm regards,

Alice Barlaam

Political Science Bachelor Student

University of Amsterdam

edss@uva.nl