Project Security 24-25 – Individueel Product



Klas: 3de jaars herkansing

Studentennaam en nummer: Enzo Gontea, 500904858

Datum: 21 januari 2025

Versie: 2

Inhoud

[Management samenvatting 3](#_Toc188362886)

[1 Inleiding 4](#_Toc188362887)

[2 Probleemstelling 5](#_Toc188362888)

[3 Gekozen Oplossing 12](#_Toc188362889)

[4 Functioneel Ontwerp Oplossing 13](#_Toc188362890)

[5 Technische Productbeschrijving 16](#_Toc188362891)

[6 Eindconclusie 19](#_Toc188362892)

[Bronnen 21](#_Toc188362893)

[Bijlage C, Logboek en Reflectie 22](#_Toc188362894)

# Management samenvatting

Dit project richt zich op de ontwikkeling van een prototype e-mailscanner die gebruikmaakt van Machine Learning, specifiek het LogisticRegression model, om phishing e-mails te detecteren. LogisticRegression is een classificatietechniek die effectief is bij het analyseren van binaire uitkomsten, zoals het onderscheid tussen phishing en non-phishing e-mails. Het doel van deze scanner is om een extra laag van bescherming te bieden tegen phishing aanvallen door e-mails te analyseren en verdachte patronen te herkennen.

Tijdens het project is gebruik gemaakt van een dataset met Engelstalige phishing e-mails, aangezien er een gebrek is aan Nederlandstalige datasets. Hierdoor is de scanner momenteel alleen toepasbaar op Engelstalige e-mails, wat geen groot probleem vormt aangezien de meeste phishing e-mails in het Engels worden geschreven.

De e-mailscanner heeft een functionele eerste versie opgeleverd, maar is nog beperkt in complexiteit en vereist verdere ontwikkeling om geavanceerde detectiemethodes te ondersteunen.

# Inleiding

In een tijdperk waarin digitale communicatie de kern vormt van vrijwel alle bedrijfsprocessen, worden organisaties steeds vaker geconfronteerd met dreigingen zoals phishing. Phishing is een cyberaanval waarbij criminelen proberen gevoelige informatie te verkrijgen, zoals wachtwoorden of financiële gegevens, door zich voor te doen als een betrouwbaar iemand in een e-mail. Ondanks de bestaande beveiligingsmaatregelen zoals spamfilters en DMARC-verificatie, slagen phishing e-mails er vaak in om traditionele detectiesystemen te omzeilen, wat ernstige gevolgen kan hebben voor de veiligheid van organisaties.

Dit rapport beschrijft de achtergrond, probleemstelling, technische aanpak en resultaten van het project. Daarnaast worden conclusies gepresenteerd en tot slot een advies aan de organisatie.

# Probleemstelling

* 1. Huidige situatie

De organisatie is een mkb-bedrijf wat opereert in de financiële sector. De kernactiviteiten omvatten het beheer van gevoelige klantgegevens, het faciliteren van digitale communicatie met klanten en partners en financiële rapportage. De organisatie heeft een centrale IT-infrastructuur en de communicatie verloopt voor het grootste deel via de e-mail. Dit is een essentieel proces binnen de dagelijkse bedrijfsvoering.

De belangrijkste processen binnen de organisatie zijn:

* Klantenservice: Medewerkers communiceren met klanten via e-mail voor aanvragen, facturen en uitwisseling van documentatie.
* Interne communicatie: Afdelingen gebruiken e-mail om taken te verdelen en updates te delen. Ook worden op deze manier projecten gecoördineerd.
* Samenwerking met externe partners: Veel communicatie met leveranciers en zakelijke partners verloopt via de e-mail, denk hierbij aan contracten of gevoelige data.

E-mail is daarmee een primaire communicatietool en een potentieel doelwit voor cyberaanvallen zoals phishing.

Afbeelding met tekst, diagram, schermopname, lijn

Automatisch gegenereerde beschrijving

De technische infrastructuur van het bedrijf:

* E-mailservers: Microsoft Exchange voor interne en externe e-mailcommunicatie. Outlook is de standaard e-mailclient.
* Beveiligingssystemen: DMARC, SPF en DKIM zijn ingesteld om te controleren of inkomende e-mails afkomstig zijn van geautoriseerde domeinen. Antivirussoftware en een firewall zorgen voor basisbescherming tegen malware.
* Gegevensopslag: Klantdata wordt opgeslagen in een centrale SQL-database, die gekoppeld is aan een CRM-systeem. De back-upsystemen zijn geautomatiseerd en worden maandelijks gecontroleerd.
* Medewerkerstoegang: Alle medewerkers hebben toegang tot e-mail via beveiligde laptops of desktopcomputers met multi-factor authenticatie (MFA).

Medewerkers maken dagelijks gebruik van het e-mailsysteem voor:

* Klantvragen te beantwoorden en gevoelige documenten zoals facturen te versturen.
* Interne afstemming te faciliteren tussen teams.
* Communicatie met externe partners in het buitenland over eventuele projecten en diensten.

Afbeelding met tekst, diagram, schermopname, Lettertype

Automatisch gegenereerde beschrijving

* 1. Probleemstelling

De organisatie is getroffen door een phishing-aanval. Ondanks de implementatie van DMARC en andere beveiligingslagen zoals SPF heeft de aanvaller toch succesvol een phishing mail kunnen versturen naar de medewerkers. Deze e-mail leek van een geautoriseerd domein af te komen. Hierdoor zijn medewerkers misleid en zijn er vertrouwelijke documenten gedeeld zoals klantinformatie en inloggegevens.

Het doelwit van de aanval waren de medewerkers van de klantenservice en de administratie. Deze afdelingen communiceren vaak met externe partijen en delen dus vaak gevoelige informatie.

De aanvaller maakte gebruik van een domein wat correct geconfigureerd was voor SPF, DKIM en DMARC waardoor technische controles geen verdachte activiteiten detecteerden. De e-mail had een dringende oproep: “Update uw wachtwoord binnen 24 uur om toegang te behouden”. Hierdoor handelden de getroffen medewerkers zonder extra verificatie. De e-mail leidde naar een pagina die sterk leek op de officiële inlogpagina van de organisatie.

De medewerkers vertrouwden op de DMARC-validatie en zagen geen indicatie van een verdachte afzender. Minstens twee medewerkers hebben op de link geklikt en hun inloggegevens ingevoerd, waardoor de aanvaller toegang heeft gekregen tot hun interne systemen.

Het e-mailsysteem (Outlook) heeft de phishing e-mail correct afgeleverd omdat deze slaagde voor DMARC-controles. In combinatie met SPF en DKIM werd DMARC omzeild doordat de aanvaller een geautoriseerd domein gebruikte.

De aanval viel plaats omdat de aanvaller gebruik maakte van een kwetsbaarheid:

1. Geregistreerd domein dat lijkt op een vertrouwd domein
2. Correcte SPF- en DKIM-configuraties (om DMARC te passeren)
3. Phishing e-mail gestuurd naar specifieke doelwitten binnen de organisatie **met** een overtuigende call-to-action
4. Medewerkers zijn naar een nagemaakte inlogpagina geleid, waar vervolgens inloggegevens zijn verzameld

De kwetsbaarheden in het proces zijn:

DMARC. DMARC beschermt voornamelijk tegen spoofing, maar niet tegen aanvallen waarbij een geldig domein wordt gebruikt.

De medewerkers. Ze vertrouwden uitsluitend op technische verificatie zonder extra controle (zoals een waarschuwing of inhoudsanalyse van verdachte e-mails)

De directe gevolgen van de aanval:

* Onbevoegde toegang tot interne systemen door gestolen inloggegevens
* Vertrouwelijke klantdata (inclusief financieel) zijn gelekt en in verkeerde handen
* Tijdelijke verstoring van interne processen, omdat IT-afdelingen toegang moesten herstellen

De indirecte gevolgen van de aanval:

* Klantvertrouwen verminderd na melding van het incident
* Reputatieschade van de organisatie binnen de sector
* Financiële schade door IT-herstelwerkzaamheden en boetes in het kader van de GDPR (bij verlies van persoonsgegevens)
  1. Gewenste situatie

De organisatie wil een oplossing implementeren die phishing-aanvallen herkent en voorkomt, zelfs als deze DMARC- en andere beveiligingsmechanismen omzeilen. Daarnaast moeten medewerkers zich ook sneller bewust zijn van verdachte e-mails. Het doel is dus om zowel technische als menselijke zwakheden in het huidige proces te versterken.

Het doel voor de technische zwakheden is een extra laag beveiliging toevoegen die verdachte inhoud in inkomende e-mails analyseert. Ook wil de organisatie de implementatie van een waarschuwingstool die medewerkers helpt om verdachte e-mails te omzeilen. De monitoring en logging moet ook verbeterd worden zodat verdachte activiteiten sneller kunnen worden gedetecteerd.

Voor de menselijke zwakheden wil de organisatie de medewerkers opleiden in het herkennen van verdachte e-mails. Ook wil de organisatie een duidelijke procedure voor het rapporteren en behandelen van verdachte e-mails.

De organisatie wil voorkomen dat phishing-aanvallen opnieuw succesvol zijn en schade veroorzaken.

Op technisch gebied betekent dit het voorkomen dat aanvallers verdachte e-mails kunnen versturen via legitiem uitziende domeinen, zelfs als deze bijvoorbeeld DMARC passeren. Ook moet de impact van een succesvolle aanval geminimaliseerd worden door een snelle detectie en respons.

Op menselijk gebied betekent dit dat medewerkers vermijden inloggegevens of andere vertrouwelijke documenten te delen via malafide websites, en vermijden dat medewerkers blindelings vertrouwen op technische validatie.

De organisatie streeft uiteindelijk naar een situatie waarin phishing-aanvallen automatisch worden gedetecteerd en gemarkeerd voordat ze medewerkers bereiken. Hierdoor kunnen de medewerkers (met de benodigde training) alert zijn en zelf ook verdachte e-mails herkennen en rapporteren.

* 1. Acceptatiecriteria

**Functionele vereisten:**

Het systeem moet verdachte e-mails kunnen identificeren op basis van afwijkingen in de informatie van de afzender, zoals taalgebruik of inhoud (tekst). Medewerkers moeten gewaarschuwd worden als een e-mail verdacht is, zelfs als deze de DMARC-controle passeert.

Het product moet gebruiksvriendelijk zijn voor niet-technische medewerkers. Medewerkers moeten een duidelijke waarschuwing krijgen, door bijvoorbeeld een verdachte e-mail te markeren of via een pop-up.

**Technische vereisten:**

Het systeem moet inhoud van e-mails scannen op verdachte elementen, zoals woorden als ‘belangrijk’ die aanroepen tot actie.

Het systeem moet voldoen aan GDPR-vereisten door geen gevoelige klantdata buiten de organisatie op te slaan of te verwerken.

Het systeem moet alle verdachte e-mails en gebruikersacties loggen voor latere analyse en rapportages genereren over de detectie van phishing e-mails en medewerkers die phishing hebben gerapporteerd.

Het product moet verdachte e-mails markeren zonder de functionaliteit van de e-mail te verstoren. Het moet medewerkers helpen bij het nemen van beslissingen over het wel of niet vertrouwen van een e-mail. Het product moet ook flexibel zijn om nieuwe phishing-tactieken te kunnen detecteren.

Het product moet niet automatisch e-mails blokkeren zonder voorafgaande validatie of waarschuwing aan medewerkers. Uitzondering op deze regel is dat voorafgaand een configuratie is ingesteld door de IT-afdeling.

Het product moet ook niet onnodige druk leggen op de bestaande infrastructuur van de IT.

* 1. Relevante wet- en regelgeving, standaarden, en richtlijnen

Algemene Verordening Gegevensbescherming (AVG/GDPR) (Autoriteit Persoonsgegevens, 2024):

De oplossing moet voldoen aan de AVG, aangezien de organisatie werkt met gevoelige klantgegevens. De belangrijkste aspecten zijn:

Dataminimalisatie, want alleen noodzakelijke gegevens mogen worden verwerkt.

Incidentmelding: Bij een datalek moet de organisatie binnen 72 uur melding doen bij de AP.

Het systeem mag geen persoonsgegevens opslaan zonder toestemming of noodzaak, en loggingfunctionaliteit moet voldoen aan de regels voor privacybescherming.

Wet bescherming bedrijfsgeheimen (Wbb) (Ondernemersplein, 2024):

De oplossing moet bijdragen aan het beschermen van bedrijfsgevoelige informatie, zoals eigendom of financiële data.

Telecommunicatiewet (Rijksoverheid, 2024):

E-mails worden beschouwd als elektronische communicatie. Het systeem mag niet e-mails blokkeren zonder toestemming, tenzij dit noodzakelijk is voor beveiligingsdoeleinden.

ISO 27001 (ISO, 2024):

De organisatie moet voldoen aan deze internationale standaard voor informatiebeveiliging, wat inhoudt dat de oplossing bijdraagt aan het beschermen van vertrouwelijkheid, integriteit en beschikbaarheid van informatie.

NIST CyberSecurity Framework (CSF) 2.0 (National Institute of Standards and Technology, 2024):

Het system moet bijdragen aan de vijf NIST-domeinen:

Identify: Identificeren van risico’s, zoals phishing-aanvallen.

Protect: Beschermen van systemen en data.

Detect: Realtime detectie van verdachte activiteiten.

Respond: Actie ondernemen bij een aanval.

Recover: Herstellen van een aanval zonder grote schade.

# Gekozen Oplossing

* 1. Advies

Na een analyse van de huidige situatie, het probleem en de gewenste situatie, wordt aanbevolen om een phishing-detectie en waarschuwingssysteem te implementeren dat gebruik maakt van Machine Learning. Deze oplossing biedt de meest effectieve aanpak om phishing-aanvallen te detecteren en medewerkers tijdig te waarschuwen, zelfs wanneer deze de DMARC-controles omzeilen.

De voorgestelde oplossing biedt een effectieve detectie van phishing e-mails aan. Zo kunnen Machine Leaning-algoritmes afwijkingen in e-mails identificeren die met traditionele technieken, zoals DMARC, niet opgemerkt worden. Het systeem analyseert meerdere kenmerken, zoals de structuur van de e-mail en het taalgebruik. Hierdoor worden complexe phishing aanvallen effectief gedetecteerd.

Het systeem markeert verdachte e-mails visueel en waarschuwt medewerkers vóórdat zij mogelijk schadelijke acties ondernemen, zoals klikken op verdachte links. Dit voorkomt dat medewerkers vertrouwen op technische validaties zoals DMARC alleen.

Het systeem kan eenvoudig worden geïntegreerd met e-mailclients zoals Microsoft Outlook, zonder grote aanpassingen aan de bestaande infrastructuur. Door medewerkers feedback te geven over waarom een e-mail als verdacht wordt beschouwd, draagt het systeem bij aan de bewustwording binnen de organisatie.

De oplossing werkt als volgt:

Het systeem gebruikt Machine Learning-modellen die getraind zijn op een dataset van legitieme en phishing e-mails. De e-mails worden gescand en beoordeeld op kenmerken zoals:

* Gebrekkig Engels. Dit komt vaak voor in phishing mails.
* Een dringende oproep (een gebruiker moet op een link klikken)
* Taalgebruik

Als een e-mail verdachte kenmerken heeft, wordt deze gemarkeerd en ontvangt de medewerker een waarschuwing.

# Functioneel Ontwerp Oplossing

* 1. Plaats binnen context, plaats binnen organisatie, relatie met gekozen oplossing en doel

De oplossing is specifiek ontworpen om de zwakke punten in de beveiliging te versterken. Deze zwakke punten ontstaan omdat de phishing-aanvallen de DMARC-controles weten te omzeilen. Phishing blijft een van de meest voorkomende cyberdreigingen, en aanvallers maken gebruik van steeds geavanceerdere technieken om medewerkers te misleiden (Groeneveld, 2017) (Trevino, 2023) (KPN, 2022). De voorgestelde oplossing pakt zowel technische als menselijke zwakheden aan en vormt een aanvulling op de bestaande beveiligingsmaatregelen van de organisatie.

De oplossing wordt geïntegreerd in de bestaande IT-infrastructuur en speelt een cruciale rol in de dagelijkse e-mailcommunicatie. Het raakt meerdere organisatorische niveaus en afdelingen:

De IT-afdeling is verantwoordelijk voor de implementatie, configuratie en onderhoud van de tool. Ook analyseert de IT-afdeling logbestanden en verdachte meldingen voor forensisch onderzoek en risicobeoordeling.

De medewerkers zijn de directe gebruikers van het systeem. Zij ontvangen de waarschuwingen en leren hoe ze verdachte e-mails kunnen herkennen en rapporteren. Hiermee wordt het bewustzijn van de phishing e-mails bevorderd.

Het management stelt beleidslijnen op en zorgt voor naleving van relevante regelgeving. Ook bewaakt het management de effectiviteit van de oplossing.

De gekozen oplossing sluit nauw aan bij het gestelde doel om phishing-aanvallen te detecteren, voorkomen en medewerkers bewuster te maken.

Machine Learning-modellen kunnen patronen herkennen die wijzen op phishing, zelfs wanneer aanvallers geavanceerde technieken gebruiken. Dit voorkomt dat verdachte e-mails ongemerkt doorgestuurd worden naar medewerkers. De oplossing markeert verdachte e-mails en voorkomt dat medewerkers slachtoffer worden van phishing.

Door waarschuwingen te bieden worden medewerkers actief betrokken in het detectieproces. Dit vergroot hun beveiligingsbewustzijn.

Door incidenten te verminderen blijft de organisatie compliant met AVG en andere wet- en regelgeving. De reputatie van de organisatie wordt beschermd door schade aan data en klantvertrouwen te minimaliseren

De nieuwe process flow binnen de organisatie na implementatie van de oplossing ziet er als volgt uit:

1. E-mailontvangst: Inkomende e-mails worden ontvangen door de mailserver.
2. Phishing-analyse: Elke inkomende e-mail wordt door de phishing-detectietool gehaald. Het algoritme scant de e-mail op afwijkende taal, of een dringende oproep.
3. Classificatie: De e-mail wordt geclassificeerd als veilig of verdacht/malafide. Bij een veilige classificatie wordt de e-mail normaal afgeleverd in de inbox, bij een malafide classificatie wordt de e-mail met een waarschuwingsbericht gemarkeerd.
4. Waarschuwing: Bij verdachte e-mails ontvangen medewerkers een waarschuwing.
5. Monitoring en optimalisatie: De IT-afdeling monitort de prestaties van de tool, verwerkt meldingen, en past het model aan op basis van nieuwe phishingtechinieken.
   1. Netwerk en Systeem diagrammen

Afbeelding met tekst, diagram, schermopname, lijn

Automatisch gegenereerde beschrijving

E-mailserver: ontvangt inkomende mails van buiten de organisatie.

Mail gateway: bestaande oplossing die validatie uitvoert met DMARC, SPF en DKIM.

Phishing-detectietool: Aanvullende oplossing die controles uitvoert op phishing indicatoren en bepaalt of een e-mail veilig of verdacht/malafide is.

IT-afdeling: monitort de phishing tool en voert forensische analyses uit.

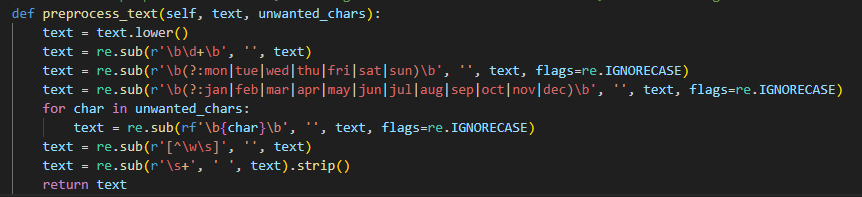
# Technische Productbeschrijving

* 1. Gebruikte tools en gerealiseerde componenten, bewijs (code) screenprints

Voor het model zelf zijn de volgende tools gebruikt:

Python. Het hele model is geschreven in Python en er zijn ook een aantal libraries van Python voor gebruikt, waaronder:

**Regex,** voor het cleanen van de data (dit kleine datacleaning script heb ik gebruikt van iemand anders) (Pinzariu, 2024):



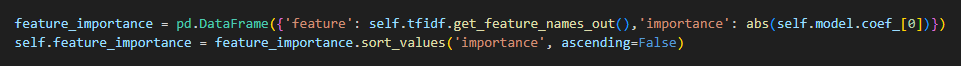
**Pandas**, voor het laden van de data en het om te zetten naar een dataframe

Afbeelding met tekst, Lettertype, schermopname, nummer

Automatisch gegenereerde beschrijving

Hier voegt pandas de samples van phishing en non-phishing mails samen. 

Hier wordt de dataframe aangemaakt op basis van de dictionary die wordt meegegeven.



**Sklearn,** voor alles omtrent het model maken

Hier wordt de data getokenized. Een model kan geen woorden lezen, maar wel getallen. Als de data omgezet wordt naar waardes, wordt dat het tokenizen van de data genoemd.

Afbeelding met tekst, Lettertype, schermopname

Automatisch gegenereerde beschrijving

Hier zoekt GridSearchCV naar de beste score op basis van de f1-score, volgens het LogisticRegression model. De geteste parameters bevinden in de param\_grid variabele. Dit is een dictionary met key value waarbij de values lists zijn. Hier worden alle mogelijke combinaties getest, en de beste score wordt gereturnd.

Afbeelding met tekst, schermopname, Lettertype

Automatisch gegenereerde beschrijving

De f1-score geeft de precisie van het model aan in het classificeren van data. Het toont ook de betrouwbaarheid van het model aan (Encord, 2023).

In de afbeelding hierboven is ook te zien dat er de module **time** wordt gebruikt. Dit was puur om te laten zien hoe snel het model wordt getraind.

En tot slot, **Pickle,** voor het opslaan van het model zodat het niet telkens opnieuw getraind hoefde te worden.

Afbeelding met tekst, schermopname, Lettertype, lijn

Automatisch gegenereerde beschrijving

Afbeelding met tekst, schermopname, Lettertype, lijn

Automatisch gegenereerde beschrijving

Er is ook een dataset gebruikt. Deze is gedownload van Kaggle, de link staat in de bronnenlijst (Alam, 2024).

De enige dataset die is gebruikt is de phishing\_email dataset. Dit waren 80.000 mails, waarvan ongeveer 40.000 spam e-mails en 40.000 legitieme e-mails.

* 1. Proces flows, software diagrammen, dialoog diagrammen, link met functioneel ontwerp

Voor de gebruikers van het product zal er niet veel veranderen. Het enige wat de gebruikers nu moeten doen is mails door een scanner halen.

Het gebruik van het product is simpel. De gebruiker kopieert de e-mail tekst en plakt deze in de terminal, en klikt vervolgens op enter. Het algoritme scant de e-mail en geeft vervolgens een classificatie op basis van de tekst, en ook hoe zeker het programma ervan is of het Phishing of Non-Phishing is.

Als een gebruiker het programma wil afsluiten, typt de gebruiker ‘quit’ in de terminal. Het programma sluit zichzelf dan af.

* 1. Technische conclusie

Om dit product te testen heb ik gebruik gemaakt van e-mails uit mijn spam folder.

De e-mail scanner werkt, maar is nog wel erg eenvoudig (barebones). Het programma heeft duidelijk meer data nodig. Ook werkt de scanner niet goed als het mails zijn van maar 1 of 2 zinnen. Dit komt omdat het model ook niet erg uitgebreid is.

Ik kon ook geen Nederlandse spam/phishing e-maildatabase vinden waardoor ik mijn code in het Engels moest schrijven. De e-mailscanner werkt dus ook alleen maar met Engelse e-mails. Dit is geen probleem aangezien de meeste spam e-mails in het Engels worden geschreven.

Er kan dus geconcludeerd worden dat de e-mail scanner werkt, maar wel beperkt. Het is een redelijke eerste versie, die wel de functionaliteiten heeft maar nog geen geavanceerde methodes. Het model scant bijvoorbeeld geen URLs, e-mailadressen of onderwerpen.

Ik heb ook uiteindelijk gekozen voor een markering van de mail (door middel van een classificatie in de terminal) in plaats van een pop-up. Ik vond dit beter voor gebruiksvriendelijkheid.

# Eindconclusie

* 1. Samenvatting Technische, Functionele en Organisatorische conclusies

**Technisch**

De e-mailscanner werkt naar behoren en is in staat om phishing e-mails te herkennen, maar is wel nog vrij eenvoudig in functionaliteit. Het gebruikte LogisticRegression model presteert redelijk maar heeft meer data nodig om de nauwkeurigheid te verhogen, vooral bij korte e-mails van een paar zinnen werkt het model niet nauwkeurig.

De huidige implementatie biedt een functionele eerste versie van een phishing e-mailscanner maar maakt geen gebruik van geavanceerde methodes (zoals bijvoorbeeld het scannen van URLs).

**Functioneel**

De oplossing biedt een basisfunctionaliteit voor het scannen en detecteren van phishing e-mails voor de medewerkers, maar mist momenteel de verfijning om alle soorten phishing effectief te herkennen.  
Het ontbreken van ondersteuning voor Nederlandstalige phishing e-mails kan worden gezien als een beperking voor organisaties die voornamelijk Nederlandse communicatie verwerken. Dit kan worden verbeterd door aanvullende datasets in integreren.

Ondanks de beperkte functionaliteit, biedt de scanner een goede basis voor verdere ontwikkeling, zoals het toevoegen van geavanceerde modellen of aanvullende functionaliteiten.

**Organisatorisch**

De huidige versie van de e-mailscanner biedt een eerste stap naar een beter beveiligde e-mailomgeving en heeft potentie om verder te worden verbeterd met meer data en verfijning van het model.

De tool is vooral nuttig voor organisaties die al veel Engelstalige communicatie ontvangen, maar zou minder effectief zijn in een puur Nederlandstalige context zonder aanpassingen.

De scanner biedt organisaties een basis waarmee ze phishing risico’s kunnen beperken, hoewel een vervolgtraject noodzakelijk is om de functionaliteit te optimaliseren.

* 1. Advies aan de organisatie

Ik adviseer de organisatie om dit model te gebruiken voor een tweede versie die meer dan alleen de tekst scant. Dit model kan veel beter werken met bijvoorbeeld een extra scan over de URL.

Ik adviseer de organisatie ook om dit model wel in gebruik te nemen waar nodig is. Ook zijn trainingen voor de medewerkers belangrijk omdat het model nog niet perfect is.

Tot slot adviseer ik de organisatie om een Nederlands model te maken voor de Nederlandse spam e-mails.

# Bronnen

Alam, N. A. (2024, April 20). *Phishing Email Dataset*. Retrieved from Kaggle: https://www.kaggle.com/datasets/naserabdullahalam/phishing-email-dataset/data

Autoriteit Persoonsgegevens. (2024, december 6). *De AVG in het kort*. Retrieved from Autoriteit Persoonsgegevens: https://www.autoriteitpersoonsgegevens.nl/themas/basis-avg/avg-algemeen/de-avg-in-het-kort

Encord. (2023, Juli 18). *F1 Score in Machine Learning*. Retrieved from Encord: https://encord.com/blog/f1-score-in-machine-learning/

Groeneveld, C. (2017, Mei 6). *Cybercrime, serieus probleem voor bedrijven*. Retrieved from Rijksoverheid: https://magazines.rijksoverheid.nl/ezk/ezkinbeeld/2017/05/06-feiten-en-cijfers#:~:text='Malware'%2C%20'ransomware',meest%20voorkomende%20vormen%20van%20cybercriminaliteit.

ISO. (2024, december 6). *ISO/IEC 27001:2022*. Retrieved from ISO: https://www.iso.org/standard/27001

KPN. (2022, September 9). *Cyberaanvallen: de 10 meest voorkomende soorten en hoe voorkom je ze?* Retrieved from KPN: https://www.kpn.com/zakelijk/blog/10-soorten-cyberaanvallen.htm

National Institute of Standards and Technology. (2024, februari 26). *The Nist Cybersecurity Framework (CSF) 2.0*. Retrieved from NIST: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

Ondernemersplein. (2024, december 6). *Bedrijfsgeheim beschermen*. Retrieved from Ondernemersplein: https://ondernemersplein.kvk.nl/bedrijfsgeheim-beschermen-wbb/

Peeters, W. (2018). *Van leerdoelen naar leeruitkomsten*. Retrieved from Vernieuwenderwijs: https://www.vernieuwenderwijs.nl/van-leerdoelen-naar-leeruitkomsten/

Pinzariu, A. (2024, November 8). *FINAL VERSION - Phishing Model*. Retrieved from Kaggle: https://www.kaggle.com/code/arianapinz/final-version-phishing-model

Rijksoverheid. (2024, december 6). *Toezicht op telecombedrijven*. Retrieved from Rijksoverheid: https://www.rijksoverheid.nl/onderwerpen/telecommunicatie/toezicht-op-telecommunicatie

Trevino, A. (2023, Augustus 30). *De meest voorkomende soorten cyberaanvallen*. Retrieved from Keeper: https://www.keepersecurity.com/blog/nl/2023/08/30/the-most-common-types-of-cyberattacks/

# Bijlage C, Logboek en Reflectie

|  |  |  |
| --- | --- | --- |
| **Datum** | **Wat heb ik gedaan?** | **Beschrijving** |
| 19 november 2024 | Onderwerp gekozen | Iets met phishing gekozen omdat ik dat nog niet eerder heb gedaan |
| 2 – 6 december 2024 | Hoofdstuk 2 uitgewerkt | Over deze dagen heb ik hoofdstuk 2 verspreid gemaakt |
| 6 december 2024 | Voorlopige versie ingeleverd | Ik heb ook al een aantal ideeën voor een oplossing bedacht |
| 20 december 2024 | 3.1 gemaakt | Oplossing gekozen |
| 21 december 2024 | 4.1 gemaakt | API opgezocht voor de email scanner |
| 22 december 2024 | 4.2 gemaakt | Toch gekozen voor een daadwerkelijke dataset downloaden in plaats van een API |
| 28 december 2024 | Data gezocht voor model | 3 datasets gevonden, alvast gemerged en gelijk gemaakt met behulp van python script |
| 1 januari 2025 | Model uitgezocht, begonnen met cleanen | Data leesbaar maken voor model voor ik het model ga trainen, toch gekozen voor maar één dataset in plaats van 3. |
| 2 januari – 12 januari 2025 | Coderen | Enorm veel tijd besteed aan het coderen, onderzoek doen en alles over de code. |
| 13 januari 2025 | Begonnen aan 5 | 5.1 gemaakt |
| 14-15 januari 2025 | 5 afgemaakt | Conclusie geschreven, kritisch geweest op mezelf |
| 16 januari 2025 | Eindconclusie + management samenvatting | Puntjes op de I, maar in principe hoef ik geen research meer te doen nu, alleen samenvattingen schrijven en conclusie. |
| 20 januari 2025 | README.md geschreven | Zowel Engels als Nederlandstalige versie |
| 21 januari 2025 | Puntjes op de i | Technische documentatie aangescherpt, inleiding opnieuw geschreven, nog een extra netwerkdiagram gemaakt, managementsamenvatting geschreven |