VEILIGE CONFIGURATIES VAN WINDOWS ENDPOINTS

Stage Portfolio

Insign.it
Fontys Hoge school ICT

Rik Leemans

STAGEPORTFOLIO VOOR FONTYS HOGESCHOOL ICT

Gegevens student(e):

R.
Rik
Leemans

Studentnummer: [redacted]

Profiel/innovatiegebied: Cyber security

Stageperiode datum van 29 augustus 2022 t/m 20 januari 2023 (5 werkdagen, 40 uur in de week)

Gegevens bedrijf:

Insign.it

Security

Venlo

[redacted]

Engineer/ support consultant

Gegevens docentbegeleid(st)er:

[redacted]

Gegevens verslag:

Veilige configuraties van Windows endpoints

Datum uitgifte stageverslag

Getekend voor gezien door bedrijfsbegeleid(st)er:

[redacted]

10-1-2023

De bedrijfsbegeleid(st)er,

Inhoud

Versie geschiedenis

Versie	Datum	Acteur	Opmerkingen
1	28-10-2022	Rik Leemans	De opdracht beschreven
2	08-11-2022	Rik Leemans	Inleiding, bedrijf en start proces en resultaten
3	09-11-2022	Rik Leemans	Start proces en resultaten
4	10-11-2022	Rik Leemans	Eerste versie proces en resultaten tot nu
5	6-12-2022	Rik Leemans	Feedback docent verwerkt.
6	7-12-2022	Rik Leemans	Bewijs competenties analyse, advies en ontwerp, realisatie
7	8-12-2022	Rik Leemans	Bewijs competenties beheer&controle, oordeel, communicatie en leervermogen
8	9-12-2022	Rik Leemans	Spelling controle
9	10-01-2023	Rik Leemans	Voorwoord

Voorwoord

Hallo, mijn naam is Rik Leemans, 21 jaar oud en kom uit Eindhoven. Afgelopen semester ben ik begonnen met de specialisatie “Cyber Security”, nu vervolg ik mijn keuze door een Cyber Security stageopdracht uit te voeren. Mijn interesse voor Cyber Security is tijdens de opleiding van Fontys vergroot. Om deze keuze en het aanbod heb ik gekozen om het project “veilige configuraties voor Windows eindpoints” aan te nemen om meer ervaring en kennis op te doen in Venlo. Met als resultaat Insign.it te helpen versterken in de veiligheid van hun Windows systemen.

Inleiding

Hoe kan je ervoor zorgen dat secure configuraties worden geïmplementeerd, zodat de werkzaamheden voor de betreffende rol/functie binnen insign.it praktisch uitvoerbaar blijven. Dit onderzoek wordt in drie fases behandeld. Een analyse fase om het onderzoek vooraf in kaart te brengen en informatie op te doen. Een implementatie fase om het te kunnen toepassen en resultaten en conflicten te behandelen. En tot slot een test fase waarin het product getest wordt op gebruik.

Het bedrijf

Insign.it is ontstaan in 2000 in Venlo, ze zijn met drie mensen begonnen en het bedrijf is nu gegroeid met een tiental medewerkers in het bedrijf. Insign.it bedenkt, ontwerpt, implementeert en beheert hun hightech infrastructuren. Deze concepten leveren ze op het gebied van werkplek, security, cloud, datacenter en hun nieuwe managed services. Insign.it was in het verleden vooral gefocust op het bedenken, ontwerpen en implementeren van infrastructuren en informatieveiligheid systemen. Nu is er veel veranderd in de infrastructuur van de meeste bedrijven zoals modern werkplek en de cloud. Hierdoor is het bedrijf zich ook meer aan het focussen op managed services waarmee je na het opzetten bij de kant in beeld kan blijven door het beheer van de infrastructuur bij te houden/monitoren.

1. De opdracht

Beschrijving

Voor Insign.it mag ik een interne opdracht maken waarin ik veilige configuraties analyseer, implementeer en uit test voor gebruik van eindgebruikers binnen Insign.it. Documentatie gaat voor medewerkers en klanten van Insign.it gebruikt worden. Binnen deze configuraties maak ik gebruik van richtlijnen die door Center for Internet Security en Insign.it zijn beoordeeld als nodige extra beveiliging op hun besturingssystem. Cyberaanvallen op bedrijven zijn toegenomen de afgelopen jaren daarom is het belangrijk dat de veiligheid binnen het bedrijf verhoogd wordt op de kans te verminderen. Er worden een aantal verschillende configuraties voor besturingssystemen gemaakt op basis van de functie/werkzaamheden en zero trust framework. Het is hierbij belangrijk dat de configuratie verbeterd wordt zodat het zero trust framework en veiligheid van apparaat zo optimaal mogelijk wordt gebruikt, zonder dat de werkzaamheden van desbetreffende functie gehinderd worden. Dit wordt toegepast voor Windows, IOS en Android apparaten die verbonden zijn met de Azure Cloud van het bedrijf.

Het Probleem

Het probleem is de stijging van cyberaanvallen die steeds vaker op bedrijven gemunt hebben. Insign.it heeft gevoelige data die ze moeten beschermen tegen de buitenwereld, deze informatie bevatten gegevens van klanten en interne informatie van insign.it voor werkzaamheden. Daarnaast heeft Insign.it ook toegang tot systemen van klanten waarvan bescherming hiervan uiterst belangrijk is. (Aantal cybersecuritybedrijven in 5 jaar tijd verdubbeld, 2021-2022)

Verder is het voor Insign.it een mooie kans op de beveiliging via de buitenkant en binnenkant te verbeteren. Voor de aanvallers wil je de beveiliging van je bedrijf zo dicht mogelijk maken, natuurlijk door firewall, virus en internet beveiliging. Maar ook wil je het apparaten en accounts van je medewerkers zo goed mogelijk beveiligen. Door iedereen alleen de rechten te geven die nodig zijn voor hun werkzaamheden verminder je de kans op een inbraak doormiddel van gebruiker accounts. Aanvallers hebben minder mogelijkheden om personen te selecteren die voldoende rechten hebben om een succesvolle aanval uit te kunnen voeren, bovendien zijn systeembeheerders vaak bewuster van mogelijke aanvallen en houden hun account beter beveiligd.
Voor medewerkers die in het bedrijf werken komen er ook nog een aantal extra maatregelen bij. Mochten medewerkers nog van een administrator account gebruik maken of hebben ze rechten die niet (horen te) gebruiken, is dit ook een kwetsbaarheid. Medewerkers met goede of slechte bedoelingen de macht over de Cloud, server of andere applicaties veranderen, verwijderen of blokkeren. Dit kan een foutje, een grap of een wraakactie van een boze medewerker.

Doel en context van opdracht

Het doel van het project is een veilige configuratie maken voor Windows, Linux en Android apparaten dat geschikt is voor desbetreffende persoon met functie. Dit wordt wanneer het getest is en beoordeeld is door de opdrachtgever van insign.it vergeleken met de huidige configuratie voor verbeteringen. Daarnaast gaat de documentatie gebruikt worden door andere medewerkers en klanten om gelijk wijze configuraties op te zetten bij klanten.

2. Proces en resultaten

In proces gaat beschreven worden hoe de planning is verlopen die was opgezet voordat de opdracht begonnen is. Hiermee ga ik reflecteren om een conclusie te kunnen trekken of de planning reëel is opgezet en ook het proces hierbij tijdens de opdracht zich aan de planning heeft voldaan. Daarnaast heeft het bedrijf en ik een verwachting van de resultaten die zijn ontwikkeld tijdens de stageperiode. Deze resultaten ga ik reflecteren om op mijn werk en producten terug te kijken en mezelf feedback te geven en te concluderen wat ik allemaal geleerd op het gebied van cyber security en professionaliteit in het bedrijf.

Plan en geplande doelen

De planning is goed verlopen, deze heb ik in drie delen verdeeld voor dit project. Ik ben begonnen met de analyse fase waarin ik mezelf drie tot vier weken de tijd heb gegeven om de opdracht uit te zoeken en informatie over het bedrijf, intune en de richtlijnen te bestuderen. Het analyse document wat een product is voor mijn opdracht heb ik binnen drie weken opgezet en onderzoek gedaan om de informatie te kunnen uitwerken. Het analyse document heb ik ook tijdens mijn implementatie fase bewerkt en updates in het project in meegenomen. Vervolgens heb ik in de laatste week die ik gepland had voor mijn analyse fase een onderzoek gedaan voor mijn implementatie document. Dit onderzoek was met doel om meer informatie te vinden over het opzetten van een Azure omgeving en voorbereidingen voor Intune. Dit was een ideale week om voor de implementatie onderzoek te doen voor de omgeving. De informatie heb ik van medewerkers in de praktijk en van informatie van internet gehaald.

Als volgend komt de implementatie fase, deze fase heb ik wat onderzoek uitgewerkt naar de omgeving waarin ik te werk ben gegaan. Ook komt er informatie aanbod over starten met Intune en apparaten, met tot slot de implementatie van de baseline en configuratie profielen. Hier heb ik mezelf zeven tot acht weken de tijd voor gegeven om deze implementatie voor te bereiden, implementeren en uitwerken in het document. Uiteindelijk is deze planning wel kloppend qua tijdsbestek aan het implementeren, maar de implementatie fase en test fase zijn met elkaar gaan kruizen. Ik heb moment gehad tijdens de implementatie fase waarin ik al een aantal testen heb uitgevoerd voor een configuratie profiel, omdat moet wachten op akkoord of op feedback van de stagebegeleider. Hierdoor was ik wel in staat om verder te werken zonder dat ik achterstand ging maken op mijn planning. (Leemans, Insign.it, 2022)

Test fase is positief geëindigd en planning is correct aangehouden. Ik heb mezelf drie weken de tijd gegeven hiervoor. Ik ben begonnen met zelf een aantal visuele testen uit te voeren en toegang tot bedrijfsmiddelen to krijgen via [redacted] Volgend ben ik het test apparaat gaan voorbereiden, voor medewerkers die gevraagd zijn om hun werkzaamheden in de vorm van een simulatie uit te voeren. Per configuratie profiel heb ik met desbetreffende medewerkers om de beurt de testen uitgevoerd. Na elke test heb ik het test apparaat reset om met de volgende medewerker van start te gaan. Tot slot ben ik bevindingen gaan noteren en heb ik een conclusie en advies gegeven.

Doel is om drie verschillende Windows configuraties te maken voor verschillende functies binnen het bedrijf Insign.it. Daarop extra een profiel voor Linux, IOS en/ of Android besturingssysteem.

Resultaten

Het resultaat van mijn stageopdracht zijn drie Windows configuraties geworden elk gebaseerd op bedrijfsfuncties om instellingen en rechten te bepalen, dit is gedocumenteerd. Daarnaast is er een opzet configuratie voor Linux gedocumenteerd en uitgewerkt in de test omgeving. Tot slot is er configuratie gedocumenteerd voor persoonlijke Android telefoons met bedrijfsprofiel. Hiervoor is ook een opzet gemaakt. Ik denk dat Insign.it de verschillen tussen hun bestaande configuraties en mijn CIS-configuraties kunnen afwegen met elkaar, omdat dit het bedrijf kan helpen voor het verbeteren van de veiligheid van eindgebruikers apparaten.

Bij deze configuraties die gemaakt zijn in Azure omgeving “Intune” behoord ook een aantal documenten. Begonnen met het analyse document waarin kennis, analyse en advies wordt gegeven over de configuraties. Het implementatie document waarin advies wordt toegepast en beargumenteerd en een ontwerp wordt beschreven. Het test document waarin realisatie wordt beoordeeld in vergelijking met het ontwerp. Door middel van deze documenten laat ik een blauwafdruk achter waarmee insign.it informatie kan terugzoeken. Daarnaast kunnen ze mijn werk voortzetten omdat maandelijks veranderingen blijven komen en je wilt up-to-date blijven. En tot slot kunnen ze deze documentatie ook gaan gebruiken om klanten te informeren wat deze richtlijnen kunnen betekenen voor hun werkomgeving.

Reflectie

Mijn reflectie op mijn project begin ik met een aantal leermomenten die ik heb gehad tijdens mijn werkzaamheden bij Insign.it. Om te beginnen bij mijn start van mijn opdracht wilde ik alle functies en medewerkers goed in kaart brengen door elke functie een medewerker te interviewen voor hun werkzaamheden uitleg. Dit was uiteindelijk niet het efficiënte manier om te beginnen met mijn opdracht dit komt omdat de meerderheid van deze medewerkers geen ICT kennis hebben en mij alleen de informatie kunnen vertellen dat al bekend is. Daarom besloten om bij dringende vragen contact op te zoeken en tussendoor hun feedback op te nemen. Ook wilde ik in het begin een benchmark gebruiken dat bedoeld was voor Windows domain infrastructuur, ik maakte te vroeg een beslissing zonder dit meteen te controleren wat Insign.it gebruikt als infrastructuur. Uiteindelijk is dit opgelost door mijn idee te pitchen omdat mijn opdrachtgever vertelde dat ze via intune hun security regelen. Wanneer de baseline en configuratie profiel waren geïmplementeerd en uitgevoerd op het apparaat waren er heel veel conflicten tussen de baseline en profiel. Dit kwam omdat sommige policies elkaar in de weg gaan zitten, als deze meerdere keren worden ingeschakeld. Achteraf handmatig kunnen oplossen in de meeste gevallen, maar dit het vooraf met wat research voorkomen kunnen worden.

Mijn reflectie op de planning die ik opgezet en gebruikt hebt is goed, ik heb wekelijks een paar keer mijn planning bijgewerkt en wijzingen doorgevoerd. Dit heb ik ook beschikbaar gemaakt voor mijn begeleiders op mijn stageplek en mijn begeleidende docent. Alles heb ik bijgehouden op Trello en verdeeld onder verschillende fases die heb tijdens mijn project.
Probleem kunnen analyseren is een belangrijk proces in je project, ik ben bezig met een probleem op te lossen voor het bedrijf in dit project. Ik heb in elk product in de scope beschreven wat het probleem is en wat het doel is om dit op te lossen.
Ook mijn kennis over Microsoft en moderne werkplekken is vergroot. Ik heb een goed beeld gekregen over wat Microsoft voor verschillende bedrijven kan betekenen, maar ook wat de eventuele nadelen zijn van een infrastructuur met de Cloud. Ook wordt security binnen het bedrijf steeds belangrijker. Ik ben veel bezig geweest met configuratie instellingen binnen Intune, hiermee overweg gaan heb ik mijn kennis het meest in vergroot. Al met al gaat dit voornamelijk over de

transitie naar een moderne werkplek, hierover ben ik veel te weten gekomen hoe dit eruit gaat zien met de omgeving Azure en Intune. Dit kan ik meenemen voor de toekomst.
De communicatie tussen het bedrijf en mij is goed verlopen. Ik had voornamelijk met vier medewerkers binnen het bedrijf contact dit gebeurde op verschillende manieren persoonlijk, email, Slack en telefonisch. Wanneer ik informatie of materiaal nodig heb ging ik daar zelf achteraan, hierbij was verantwoordelijkheid en zelfstandigheid belangrijk. Medewerkers van insign.it stonden hiervoor altijd beschikbaar zolang je er zelf mee komt, samenwerking bij insign.it staat centraal en ik heb geleerd dat dit in een werkomgeving nog steeds erg belangrijk blijft. Ook had ik wekelijks of om de week contact met mijn begeleidende docent. Ik stelde hem op de hoogte van mijn vooruitgang en hij gaf mij feedback. Motivatie vind ik hierbij erg belangrijk zo lang je gemotiveerd bent blijf je leergierig en wil je jezelf blijven ontwikkelen, dat is tijdens deze stageopdracht zeker gelukt.

3. Bewijs voor competenties

In bewijs voor competenties gaat aangetoond worden hoe elk dimensie is behaald door onderzoeksvragen te beantwoorden. Ik refereer naar gemaakte producten waarin ik bewijs laat zien.

Analyse/Probleem definitie

Onderzoeksvraag 2: Welke rollen/functies zijn er aanwezig binnen Insign.it?

Er zijn in totaal twintig verschillende rollen/functies aanwezig binnen insign.it, na een interview met de CTO van Insign.it heb ik voor al deze rollen/functies een contactpersoon erbij gevraagd. Na nader onderzoek voor de werkzaamheden per rol/functie heb ik een overzicht in Excel wat aangeeft waar de werknemers gebruik van maken. Dit is terug te vinden in hoofdstuk 1 van Het analyse document.

Onderzoeksvraag 4: Welke secure richtlijnen zijn er die veilig toegepast zouden kunnen worden?

Ik heb drie verschillende richtlijnen gevonden waarmee je de veiligheid van je bedrijf kan verbeteren. Als eerste Microsoft security Baseline, verder CIS (center for internet security) en STIG (Security technical implementation guides). Uiteindelijk wilde insign.it verder gaan met CIS-implementatie [redacted], omdat deze richtlijn het best past bij insign.it. Analyse hierover is te vinden in hoofdstuk 2 en 3 van het analyse document.

Meer analyse over het veilige configuratie opties en de mogelijkheden van tools die gebruikt kunnen worden voor de implementatie van de richtlijnen, zijn te vinden in hoofdstuk drie van het analyse document.

Meer probleemdefinitie in elke inleiding van een document product. Ik begin met in inleiding waarom, het probleem, het doel en een procesbeschrijving.

Advies

Onderzoekvraag 3: Welke verschillende configuraties gaan er nodig zijn om elke medewerker van het juiste te voorzien?

Er zijn drie verschillende configuraties nodig om de medewerkers van insign.it te voorzien van alle benodigdheden. Uitgelegd wat de verschillen zijn tussen deze configuraties is terug te vinden in het implementatie document bij de koppen standaardgebruiker, service desk medewerker en local admin. Hoe de verschillende rollen/functies van medewerkers van insign.it zijn verdeeld staat in het analyse document bij het hoofdstuk eind keuze.

In het analyse document heb ik een afweging gemaakt voor het belang van insign.it, waarom insign.it de keuze moet maken voor [redacted]. En welke [redacted] het best bij het bedrijf past om toegepast te worden in intune. Dit wordt beschreven in eind keuze van het analyse document, hierbij ook de voordelen waarom deze keuze gemaakt is.

In het implementatie document staat in hoofdstuk “Keuze en verandering” afwegingen van belangen voor insign.it. Tijdens het implementeren is het mogelijk dat er veranderingen plaatsvinden, de wijzigingen voor implementatie en de voordelen heb ik als nieuwe mogelijkheden beschreven. Tot slot heb ik hoofdstuk 1.5.1, 1.5.2 en 1.5.3 conflicten en conclusies verwoord, waarom de overweging is gemaakt om policies en instellingen op mijn advies te gebruiken. Dit advies heb ik gebaseerd op basis van de configuratie profielen dat bij insign.it past.

Ontwerp

Het implementatie document geeft mijn ontwerp voor een veilig configuratie voor medewerkers van insign.it het best weer. Op basis van mijn keuzes en het analyse document ben ik begonnen met een test omgeving op te zetten wat insign.it ook gebruikt. In hoofdstuk 1.2, 1.3 en 1.4 laat ik zien hoe het ontwerp eruitziet en wat hiervoor nodig om het op te zetten. Op basis van het advies heb ik een

ontwerp beschreven wat elk werknemers per configuratie nodig heeft om hun werkzaamheden ongestoord te kunnen blijven uitvoeren. Dit staat beschreven onder medewerkers benodigdheden in hoofdstuk 1.5.1, 1.5.2 en 1.5.3.

Realisatie

Onderzoeksvraag 1: Hoe kunnen we ervoor zorgen dat veilige configuraties worden geïmplementeerd zodat de werkzaamheden voor de betreffende rol/functie binnen Insign.it praktisch uitvoerbaar blijven?

Dit is mogelijk door een passende configuratie te maken per rol/functie binnen insign.it. Om deze configuraties veilig te boordelen maak ik gebruik van de [redacted] die gecertificeerd veilig worden gekeurd. De werkzaamheden moeten praktisch uitvoerbaar blijven, na onderzoek naar werkzaamheden heb ik [redacted]configuraties samengesteld waarin dit voor de medewerkers mogelijk is. Deze configuraties zijn terug te vinden als admx file en in de demo van mijn presentatie.

Ook zijn deze eindproducten terug te vinden in mijn Microsoftaccount test omgeving. Door middel van Azure portal is het mogelijk om bij intune te komen, hier zijn de configuraties gevestigd. Deze zijn getest door medewerkers in het test document.

Beheer & controle

Als werkwijze heb ik gebruik gemaakt de [redacted], dit was een eis van de opdrachtgever. In het implementatie document hoofdstuk 1.5 gebruik ik constant deze richtlijnen en geef ik aan waarom het belangrijk is dat deze worden toegepast. Op een professional manier heb ik deze toegepast in Intune, waardoor het mogelijk is om de configuratie uit te voeren op drie verschillende apparaten. Door middel van deze manier blijft het overzichtelijk en beheersbaar. Insign.it heeft zelf hun omgeving in Intune, waardoor het mogelijk is om de configuraties te exporteren of de test omgeving over te nemen. Hiervoor heb ik gekozen omdat er voor Windows altijd security updates blijven komen.

Oordeel

In mijn projectplan heb ik onderzoeksvragen genoteerd, deze bevat een hoofdvraag en deelvragen. Daarnaast heb ik in het projectplan het DOT framework toegepast om een strategie en methode te bepalen hoe ik deze vragen wil uitwerken. Dit is terug te vinden in hoofdstuk 1.8 en 1.8.1.
In analyse, implementatie en test document(hoofdstuk 5) zijn deze methodes uitgewerkt. Om deze documenten betrouwbaarheid te garanderen heb ik bronnen en illustraties gebruikt.

Communicatie

Communicatie heb ik regelmatig gehad met mijn stagebegeleider, opdrachtgever en andere engineers. Ik heb documenten en gespreken waarin ik mijn voortuitgang, feedback en planning bespreek. Deze communicatie is zowel mondeling als online geweest. Ook heb ik samengewerkt om tot een juiste conclusie te komen, wanneer er een beslissen genomen moest worden. Ook heb ik regelmatig contact gehad met docentbegeleider over mijn vooruitgang. Dit is terug te vinden in communicatie document.

Leervermogen

In deze stageperiode heb ik veel kennis opgedaan in Azure AD/Intune ik ben hierin meer te weten gekomen en heb mezelf ontwikkeld in endpoint beveiliging voor verschillende besturingssystemen. In heel hoofdstuk 1 van het implementatie document heb ik hierin gewerkt. Moderne werkplekken bestaan uit hybride werkomgeving met een gepersonaliseerd account (apps, zerotrust, cyberveiligheid), hiervoor heb ik een deel onderzocht en uitgewerkt in vorm van een configuratie. Dit bestaat uit een aantal kenmerken dat ik heb beschreven in 1.1, 3.1 en 3.2.4 van het analyse document.

Een aantal professionele talenten dat ik ontwikkeld heb is zelfstandigheid en samenwerking in bedrijfsvorm. Mijn opdracht heb ik zelfstandig uitgevoerd dus ik moet zelf initiatieven nemen, planning bijhouden, updates geven en beslissingen nemen. Maar natuurlijk heb ik ook een samenwerking tussen andere medewerkers. Ik heb hulp gehad, vragen, overleg met opdrachtgever en op juiste manier zakelijk contact houden om samen tot een beter eindresultaat te komen.
Tot slot heb ik bij mijn opdrachtgever ook om feedback gevraagd, zodat ik mijn proces kan verbeteren voor de producten die ik gemaakt heb. Dit kan ik natuurlijk ook meenemen voor de toekomst. Feedback heb ik meegenomen in mijn communicatie document. Om te laten zien dat ik ook hiervan ook geleerd heb reflecteer ik mezelf ook. In dit document heb ik mijn zelfreflectie beschreven.

4. Samenvatting

Stageopdracht is positief beëindigd, door de uitkomt onderzoek en resultaten is door Insign.it besloten verder te gaan met de productie van [redacted] Dit geldt niet alleen [redacted]toepassen op Windows apparaten, maar ook de start op mobile apparaten. Door het uitvoeren van deze stageopdracht ben ik meer te weten gekomen, waarom het belangrijk is om de veiligheid van je eindpoints te blijven verbeteren. Maar ook wat de impact is op het bedrijf en haar werknemers, wanneer er richtlijnen worden toegepast. Ik heb door middel van de stageopdracht van Insign.it een beeld gekregen hoe een project loopt in een professional bedrijfsomgeving, en hoe je een samenwerking aan gaat met andere medewerkers.

5. Verklarende woordenlijst

managed services: Het uitbesteden van IT gerelateerde diensten beheerd door ICT bedrijf.

policy	: regel of beleid waaraan een apparaat aan moet voldoen.
intune	: Vernieuwede versie van admin endpoint manager een Microsoft service.
ADMX file	: bestandtype wat (group)policies instellingen kan opslaan, ex- importeren.

Bibliografie

Aantal cybersecuritybedrijven in 5 jaar tijd verdubbeld. (2021-2022). Opgehaald van KVK: https://www.kvk.nl/over-kvk/media-en-pers/nieuws-en-persberichten/--aantal-cybersecuritybedrijven-in-5-jaar-tijd-verdubbeld/#:~:text=Nederlandse%20bedrijven%2C%20groot%20en%20klein,om%20hun%20bedrijf%20te%20beschermen.

Leemans, R. (2022, 10 11). *Insign.it*. Opgehaald van Trello: https://trello.com/b/PkVrCjrS/insignit