

Project Security Individueel Product 23-24

Datalekken



(KVK, 2021)

Klas: IC202
Naam: Nilas Meeder
Studentnummer: 500908274
Datum: 13-12-2023
Versie:1.0

Inhoudsopgave

1	Doel	3
1.1	Problematiek, vereisten en doel	3
1.2	Context of situatie van de problematiek	5
1.3	Gekozen aanpak	7
1.4	Security aspecten en kwaliteitscriteria	8
2	Oplossing	10
2.1	Mogelijke oplossingen	10
2.2	Gekozen oplossing	11
2.3	Netwerk en Systeem diagrammen.	12
2.4	Kwaliteitscriteria en risicomitigaties.	13
3	Proof of Concept	15
3.1	Gebruikte tools en ontwerp	15
3.2	Proces flows, software diagrammen, dialoog diagrammen	16
3.3	Gerealiseerde componenten	17
3.4	Testen van Technisch product	18
3.4.1	Testen:	18
3.5	Proof of Context conclusie.	23
4	Eindconclusie	23
4.1	Conclusie	23
4.2	Advies en aanbevelingen.	24
5	Verwijzingen	25
	Bijlage A, Logboek en reflectie	26
	Bijlage B, optioneel	28

1 Doel

1.1 Problematiek, vereisten en doel

In dit project staat de problematiek van datalekken centraal. Met de grote toename van het aantal werknemers dat vanuit huis of andere plekken werkt, is het risico op het lekken van gevoelige bedrijfsinformatie aanzienlijk toegenomen. Zo is het gemiddelde aantal thuiswerk/ niet kantoor uren van 2,7 uur naar 7 uur per week gestegen sinds de COVID-19 pandemie (TNO, 2023). Hackers zoeken voortdurend naar mogelijkheden om misbruik te maken van deze nieuwe werkomgeving en proberen ongeautoriseerde toegang te verkrijgen tot bedrijfsnetwerken en gevoelige data. Zo is ook het aantal datalekken verdubbeld door dat mensen vanuit huis werken sinds de COVID-19 pandemie (Murat, Kose, Bastug, & Kucukkaya, 2023).

Bij een datalek gaat het om toegang tot of vernietiging, wijziging of vrijkomen van persoonsgegevens bij een organisatie, zonder dat dit de bedoeling is van de organisatie. Het gaat dus niet alleen om het vrijkomen (lekken) van gegevens, maar ook bijvoorbeeld om onrechtmatige verwerken van gegevens. Voorbeelden zijn een kwijtgeraakte USB-stick met persoonsgegevens, een gestolen laptop of een inbraak in een databestand door een hacker. Daarnaast is er sprake van een datalek wanneer er een inbreuk is op de beveiliging van persoonsgegevens, zoals beschreven in artikel 13 van de Wet bescherming persoonsgegevens. Kortom, persoonsgegevens zijn blootgesteld aan verlies of onrechtmatige verwerking, en dat is precies waar de beveiligingsmaatregelen tegen moeten beschermen (Martijn Broekhof, 2023) (AP, z.d).

Volgens het Autoriteit Persoonsgegevens (AP) zijn er 3 soorten datalekken (AP, z.d):

1. **Inbreuk op de vertrouwelijkheid:** persoonsgegevens zijn openbaar gemaakt of er is toegang geweest tot persoonsgegevens. Dit is gebeurd door iemand die daartoe niet bevoegd is. Of dit is per ongeluk gebeurd.
2. **Inbreuk op de integriteit:** persoonsgegevens zijn gewijzigd door iemand die daartoe niet bevoegd is. Of dit is per ongeluk gebeurd.
3. **Inbreuk op de beschikbaarheid:** de organisatie waar het datalek is (geweest) kan niet meer bij de persoonsgegevens komen. Of de gegevens zijn vernietigd. Dit is gebeurd door iemand die daartoe niet bevoegd is. Of dit is per ongeluk gebeurd.

Vaak werken werknemers met cloud applicaties zoals Amazon en Microsoft 365. Beperkte controle over de informatie kan verschillende veiligheidsproblemen en bedreigingen met zich meebrengen, zoals gegevensinbreuk, onbetrouwbare connectiviteit, delen van middelen (resources), toegankelijkheid van gegevens en insider aanvallen. Een schending van de beveiliging kan leiden tot onopzettelijke of onwettige vernietiging, verlies, wijziging, ongeoorloofde openbaarmaking van, of toegang tot, persoonsgegevens die worden verzonden, opgeslagen of anderszins verwerkt. (R & E. A., 2017) Datalekken komen in vele

soorten maten en manieren en hoeft niet eens altijd een kwaadwillende achter te zitten.

Vereisten

Er zijn veel verschillende vereisten die kunnen zorgen voor een datalek binnen een bedrijf.

1. Onveilige netwerkverbindingen:

- Onvoldoende beveiligde VPN's of openbare Wi-Fi-netwerken kunnen de deur openzetten voor ongeautoriseerde toegang tot bedrijfsinformatie.

2. Onvoldoende encryptie van gegevens:

- Gebrek aan encryptie bij het verzenden, opslaan en verwerken van gegevens kan leiden tot blootstelling en ongeautoriseerde toegang.

3. Onbeheerde eindpuntapparaten:

- Onvoldoende beveiliging zoals antivirus of moeilijke wachtwoorden op laptops, smartphones en andere apparaten die externe toegang hebben, kan leiden tot gegevenslekken als deze apparaten verloren gaan, gehackt of gestolen worden.

4. Onjuist gebruik van cloudservices:

- Onvoldoende beveiligingsmaatregelen bij het gebruik van cloudapplicaties kunnen leiden tot ongeautoriseerde toegang tot bedrijfsgegevens.

5. Gebrekkige authenticatieprocessen:

- Zwakke wachtwoorden, onvoldoende authenticatiemethoden en onjuist geconfigureerde toegangscontroles kunnen de kans op ongeautoriseerde toegang vergroten.

6. Onvoldoende bewustzijn en training:

- Gebrek aan training en bewustzijn bij werknemers over cybersecurityrisico's kan leiden tot onbedoeld lekken van gevoelige informatie. Zoals bijvoorbeeld met een phishing aanval.

7. Onvoldoende updates en patching:

- Niet up-to-date zijn met beveiligingspatches en updates vergroot het risico op kwetsbaarheden die kunnen worden misbruikt.

8. Insider Threats:

- Onvoldoende bescherming tegen interne bedreigingen, zoals ontevreden werknemers of personen met toegang tot gevoelige informatie.

Doel

Het doel bij een datalek heeft één doel. Gevoelige informatie beland in handen van iemand die niet bij die gevoelige informatie hoort te kunnen komen, of een bedrijf of persoon die gevoelige data beheert kan die data niet meer beheeren doordat het is vernietigd of aangepast doordat beveiliging maatregelen niet goed zijn toegepast. Zo hebben we al eerder besproken dat er 3 soorten verschillende data lekken zijn, inbreuk op de **vertrouwelijkheid**, **intergriteit** en de **beschikbaarheid** (AP, z.d).

Als een hacker achter een datalek zit blijft het doel het zelfde, gevoelige informatie beland in de handen van een persoon (De hacker) die niet bij die gevoelige informatie hoort te komen. Echter kunnen hackers wel bepaalde motieven hebben om bij die gevoelige informatie te willen komen. Meestal zijn er financiële motieven om data te lekken, dit kan onder meer betrekking hebben op het stelen van gebruikersnamen, wachtwoorden, adres gegevens, creditcardinformatie en bankrekeninggegevens. Er zijn meerdere redenen waarom hackers achter deze informatie willen komen. Met het gebruik van deze gegevens zouden frauduleuze transacties, of identiteitsfraude gepleegd kunnen worden. Heel vaak verkopen hackers dus databases met informatie die ze uit een datalek hebben verkregen aan partijen die dus aan identiteitsfraude en frauduleuze transacties willen uitvoeren. Ook kunnen hackers of kwaad willende door het gebruik van de verkregen/gelekte data proberen om mensen of organisaties te chanteren voor weer financiële doeleinden. Als de hacker van een datalek zelf deze illegale activiteiten zouden uitvoeren is de kans groter dat ze sneller gepakt worden daarom verkopen ze deze informatie op plekken zoals bijvoorbeeld het darkweb.

1.2 Context of situatie van de problematiek

Manpower is een internationaal uitzendbedrijf met een belangrijke aanwezigheid in Nederland. In Nederland opereert Manpower als een leidende dienstverlener op het gebied van arbeidsbemiddeling, flexibele arbeid en HR-oplossingen. Het bedrijf vervult de rol als een verbindende schakel tussen werkzoekenden en werkgevers, waarbij het zich richt op het matchen van geschikte kandidaten met diverse vacatures in verschillende sectoren en industrieën.

Manpower Nederland biedt een breed scala aan personeelsdiensten, waaronder tijdelijk werk, vaste banen, projectmatige opdrachten en talentontwikkeling. Het bedrijf streeft ernaar om zowel werkzoekenden als werkgevers te ondersteunen in het realiseren van hun doelen op het gebied van werk en personeelsbeheer (Manpower, z.d).

Manpower Nederland is een deel van ManpowerGroup. ManpowerGroup (vroeger bekend als Manpower Inc.) is door Elmer Winter en Aaron Scheinfeld opgericht in 1948 in Milwaukee, Wisconsin, in de VS waar ook het hoofdkantoor zich bevindt. ManpowerGroup het op twee na grootste uitzendbedrijf ter wereld (manpowergroup, z.d)

Situatie

Bij Manpower Nederland blijkt het dat het administratiesysteem waarmee Manpower werkt, genaamd "Flexservice," waarin gegevens van medewerkers en uitzendkrachten worden opgeslagen, ernstige beveiligingslekken vertoont. Een voormalige medewerker van Manpower onthult dat het systeem, dat onder andere persoonlijke informatie zoals CV's, diploma's, cijferlijsten en paspoortgegevens bevat, zo 'lek is als een zeef.' Volgens de oud medewerker waren alle gegevens van gedetacheerde medewerkers, uitzendkrachten, zzp'ers en doorleners inzichtelijk voor werknemers die niet noodzakelijkerwijs uit hoofde van hun rol of functie van die gegevens kennis behoefden te nemen. Zij hadden via de softwaresysteem eenvoudig toegang tot die gegevens. Het was zelfs mogelijk om via Flexservice de persoonsgegevens van interne medewerkers te raadplegen (Vanmorgen, 2023).

Wat nog zorgwekkender is, is dat enkele maanden voor dit incident een ander aanzienlijk beveiligingsprobleem aan het licht kwam. Bij Manpower is een significante verschuiving naar thuiswerken en werken op andere locaties plaatsgevonden. Een Administratie medewerker, die regelmatig vanuit diverse locaties zoals koffiehuisen en co-working spaces werkt, maakt vaak verbinding met onbeveiligde openbare wifi-netwerken.

Deze onbeveiligde netwerken vormen een broeinest voor cyberaanvallen, zoals man-in-the-middle (MITM) aanvallen. In dit specifieke geval heeft een cybercrimineel, door de hack techniek SSL/TLS stripping te gebruiken de HTTPS-verbinding gedowngraded naar een onbeveiligde HTTP-verbinding. Hierdoor kon de cybercrimineel de gegevens onderscheppen die werden verzonden tussen de laptop van de werknemer en de servers van Manpower. Deze gegevens waren het wachtwoord en de gebruikersnaam waarmee de werknemer kan inloggen op Flexservie. Doordat de cybercrimineel nu deze gegevens in handen had resulteerde dat in een ongeautoriseerde toegang tot het administratie systeem Flexservice waar Manpower gebruik van maakt. Alle gevoelige informatie over werknemers, uitzendkrachten en interne communicatie was daarin te vinden.

De combinatie van het eerdere datalek door onbeveiligde wifi-netwerken en de falende toegangscontrole van Flexservice heeft aanzienlijke gevolgen gehad voor Manpower. Het heeft niet alleen geleid tot verlies van vertrouwen bij klanten, juridische uitdagingen en financiële verliezen, maar heeft nu ook de gevoelige gegevens van medewerkers en uitzendkrachten blootgesteld aan ongeautoriseerde toegang en misbruik.

1.3 Gekozen aanpak

De datalekken bij Manpower Nederland is zorgwekkend en heeft al aanzienlijke gevolgen gehad voor het bedrijf. Hieronder volgt een aanpak voor het oplossen van dit probleem, waarbij een technisch product wordt ontwikkeld om de beveiliging te verbeteren en de risico's van datalekken te minimaliseren.

Er zijn 2 fases voor Manpower voor de aanpak van deze datalek.

Fase 1 is kijken naar de ernst van de situatie en de situatie in kaart brengen. Ook komt het analyseren van wat er precies fout is gegaan aan tafel. Hiervoor heeft het AP een stappenplan gemaakt voor organisaties als er een datalek is plaatsgevonden (AP, z.d).

Stap 1:

- Overzicht op de situatie creëren.

Stap 2:

- Onmiddellijk maatregelen nemen om het datalek te stoppen en de schade van het datalek te beperken en daarbij ook de risico's inschatten.

Stap 3:

- Bepaal of u het datalek wel of niet moet melden aan de AP. Zo ja, doe dit dan onmiddellijk.

Stap 4:

- Bepaal de slachtoffers wel of niet moet geïnformeerd over het datalek moeten worden. Zo ja, doe dit dan zo snel mogelijk.

Stap 5:

- Het datalek in de interne datalekregister registreren.

Fase 2 houdt in dat er een technische oplossing zal gemaakt worden. Bij een datalek is er niet een specifieke oplossing die als oplossing kan functioneren omdat datalekken in velen maten en soorten komen en vaak gepaard komen met verschillende beveiliging maatregelen die gefaald zijn, daarom is het van noodzaak om eerst te kijken naar de kwetsbaarheden en waar het fout is gegaan zodat er dan een oplossing gemaakt kan worden voor de kwetsbaarheden en het probleem. Hiervoor bied fase 1. In het geval van Manpower houdt dat in dat er een Versterking van Netwerkbeveiliging moet plaatsvinden en een versterking van de zwakheden in Flexservice. Omdat hier voornamelijk de zwakheden zitten waar de cybercrimineel heeft van kunnen profiteren.

1.4 Security aspecten en kwaliteitscriteria

Security Aspecten

Bij het aanpakken van de beveiligingsproblemen van Manpower Nederland, vooral in relatie tot het gebruik maken van onbeveiligde netwerken en het onjuist toegangscontrole in Flexservice moeten we verschillende security aspecten van deze datalek onderzoeken.

Technische aspecten:

Aanvalsmethodieken:

- **SSL/TLS Stripping:** In de aanval werd SSL/TLS Stripping gebruikt om de beveiligde HTTPS-verbinding te downgraden naar een onbeveiligde HTTP-verbinding. Dit is een techniek waarbij een aanvaller de communicatie tussen de client en de server manipuleert, waardoor de beveiliging wordt omzeild en de dataoverdracht kwetsbaar wordt voor onderschepping (Gitlan, 2023). Hierdoor kon de cybercrimineel de gebruikersnaam en het wachtwoord in handen krijgen.

Toegangscontrole:

- Het Flexservice-systeem vertoonde ernstige beveiligingslekken, waaronder een slechte toegangscontrole. Dit houdt in dat medewerkers toegang hadden tot gevoelige gegevens waarvoor zij niet geautoriseerd waren.
- De gebrekkige beveiligingsmaatregelen binnen Flexservice, zoals onvoldoende bescherming tegen ongeautoriseerde toegang, maakten het systeem kwetsbaar voor datalekken en misbruik.

Financiële aspecten:

- Een datalek kan zowel onmiddellijke als langdurige financiële gevolgen hebben. Volgens een rapport van PayPal in 2023 bedragen de wereldwijde gemiddelde kosten van een datalek \$4,45 miljoen, een stijging van 15% in de afgelopen drie jaar. Dit omvat kosten voor incidentrespons, gegevensherstel, verlies van verkopen, mogelijke uitvaltijd, en de kosten voor het versterken van het beveiligingssysteem na de inbreuk (PayPal, 2023). Voor kleine en middelgrote bedrijven kan een datalek bijzonder verwoestend zijn. Deze bedrijven besteden gemiddeld \$2,65 miljoen aan een datalek, wat neerkomt op \$3.533 per werknemer. Voor grotere organisaties zijn de kosten lager per werknemer, maar de totale financiële impact is aanzienlijk hoger (OldNational, 2019).

Dit zou betekenen dat het gebruik van een incidentrespons, gegevens herstellen, verlies van verkopen, mogelijke uitvaltijd en de kosten voor het versterken van het beveiligingssysteem na een inbreuk behoorlijk kostbaar kan zijn op de financiën van Manpower. Daarnaast zijn er ook juridische kosten zoals schadevergoedingen en boetes die kunnen afhangen van de grootte van het lek, de soort gestolen gegevens, de industrie, en de initiële reactie van Manpower op de Datalek.

Juridische aspecten

- In het geval van deze datalek bij Manpower zijn er belangrijke juridische gevolgen. Volgens de Europese en Nederlandse wetgeving, voornamelijk de Algemene Verordening Gegevensbescherming (AVG) moet een datalek worden gemeld bij de toezichthoudende autoriteit, zoals de Autoriteit Persoonsgegevens in Nederland, als er een risico is voor de rechten en vrijheden van natuurlijke personen. Als het risico hoog is, moeten ook de betrokken personen geïnformeerd worden. Verder kan een datalek leiden tot boetes door de toezichthouder en tot de verplichting van het betalen van schadevergoeding aan de betrokken personen. Daarom is het in de praktijk belangrijk om de beveiliging van persoonsgegevens voortdurend hoog op de agenda te hebben staan en om bewustzijn over privacy te bevorderen (VDB Advocaten Notarissen, 2021).

Kwaliteitscriteria

Deze vastgestelde kwaliteitscriteria zijn essentieel voor de effectiviteit van de technische oplossing voor Manpower:

1. **Beveiliging en Gegevensbescherming:**
 - De oplossing moet prioriteit geven aan het voorkomen van ongeautoriseerde toegang en datalekken.
2. **Beschikbaarheid en Betrouwbaarheid:**
 - De oplossing moet altijd beschikbaar zijn voor geautoriseerde gebruikers
 - De oplossing moet beveiligd zijn tegen diverse aanvallen en storingen.
3. **Reactietijd en Systeemprestaties:**
 - Snelle reactietijden voor gebruikersinteracties.
 - Efficiënte verwerking van gegevens zonder significante vertragingen.
4. **Onderhoud en Schaalbaarheid:**
 - Eenvoudig te onderhouden en te updaten systeem.
 - Flexibiliteit om te schalen naarmate de behoeften van de organisatie veranderen.
5. **Gebruikersvriendelijkheid:**
 - Intuïtieve interface voor zowel beheerders als eindgebruikers.
 - Heldere documentatie en ondersteuning.
6. **Compliance met Wet- en Regelgeving:**
 - Voldoen aan relevante privacywetgeving, zoals de AVG.
 - Implementatie van processen voor naleving en monitoring.

2 Oplossing

2.1 Mogelijke oplossingen

Zoals in hoofdstuk een is besproken zijn er vele soorten en maten van een datalek die gepaard komen met verschillende beveiliging maatregelen die gefaald hebben. Daarom kijken we nu in het geval van Manpower welke oplossingen er zijn tegen de manier hoe deze datalek heeft kunnen ontstaan. We kijken hier naar technische oplossingen die met name kijken naar de onbeveiligde wifi-netwerken en tegen de aanval SSL/TLS stripping.

1. **VPN:** Een VPN (Virtual Private Network) versleutelt alle gegevens die over een netwerk worden verzonden, waardoor het risico op MITM aanvallen zoals SSL/TLS-stripping wordt verminderd. Een VPN biedt een extra versleutelde laag waardoor de hacker zelfs bij een geslaagde SSL/TLS stripping aanval de versleutelde gegevens ziet (Kaspersky, z.d). Deze oplossing is vooral nuttig voor werknemers die op afstand werken en verbinding maken met onbeveiligde openbare wifi-netwerken. Echter zijn er wel nogsteeds nadelen en risico's:
 - Ook al zou de hacker bij het Gebruik van een VPN dan misschien geen SSL/TLS aanval kunnen uitvoeren een onbeveiligd netwerk blijft onbeveiligd en er zouden altijd andere aanvallen in een onbeveiligd netwerk uitgevoerd kunnen worden.
 - Ook zou het implementeren van deze oplossing zeer kostbaar zijn.
2. **IP Whitelisting:** Bij IP whitelisting wordt alleen toegang aan het systeem of netwerk gegeven aan IP adressen die in de 'witte lijst staan' en daarbij vertrouwd zijn. Door alleen bepaalde IP-adressen toe te staan om toegang te krijgen tot het netwerk of systeem of specifieke delen ervan, kan het risico van ongeautoriseerde toegang aanzienlijk worden verminderd. Deze aanpak is vooral effectief in gecontroleerde omgevingen, waar de toegang tot netwerken en systemen strikt moet worden beheerd. Een nadeel van deze oplossing:
 - In het geval van Manpower zou dat betekenen dat medewerkers dus alleen vanuit huis kunnen werken met hun vertrouwde IP adres waarvan Manpower op de hoogte is en dus niet meer vanuit bijvoorbeeld een café kunnen werken waarbij ze op een onbeveiligd netwerk zitten aangesloten.
3. **HSTS (HTTP Strict Transport Security):** Om SSL/TLS Stripping-aanvallen in onbeveiligde netwerken, zoals waar Manpower mee werd geconfronteerd, te voorkomen, is het gebruik van HTTP Strict Transport Security (HSTS) een effectieve oplossing. HSTS is een webbeveiligingsbeleid dat webbrowsers instrueert om uitsluitend veilige TLS/SSL-verbindingen te gebruiken. Dit voorkomt dat cybercriminelen webverkeer onderscheppen en de verbinding degraderen naar HTTP..Wanneer HSTS is ingeschakeld, zullen browsers automatisch alle onveilige HTTP-verzoeken naar HTTPS upgraden, waardoor end-to-end encryptie wordt gegarandeerd. Deze aanpak helpt de risico's van SSL Stripping-aanvallen te beperken door te zorgen dat de browser zich de noodzaak van een veilige verbinding naar

de site herinnert en direct naar HTTPS leidt, zelfs als een gebruiker een HTTP-URL invoert. Echter zitten hier wel een paar risico's aan:

- HSTS beschermt alleen gebruikers die al eerder een veilige verbinding met de website hebben gemaakt. Bij een eerste bezoek of na het wissen van de cache kan een gebruiker nog steeds kwetsbaar zijn voor SSL/TLS-stripping.
- Oudere browsers en telefoon's ondersteunen mogelijk geen HSTS, wat gebruikers van deze browsers blootstelt aan risico's

Er zijn nog meer risico's die hiermee kunnen komen maar dit zijn de belangrijkste in het geval van Manpower

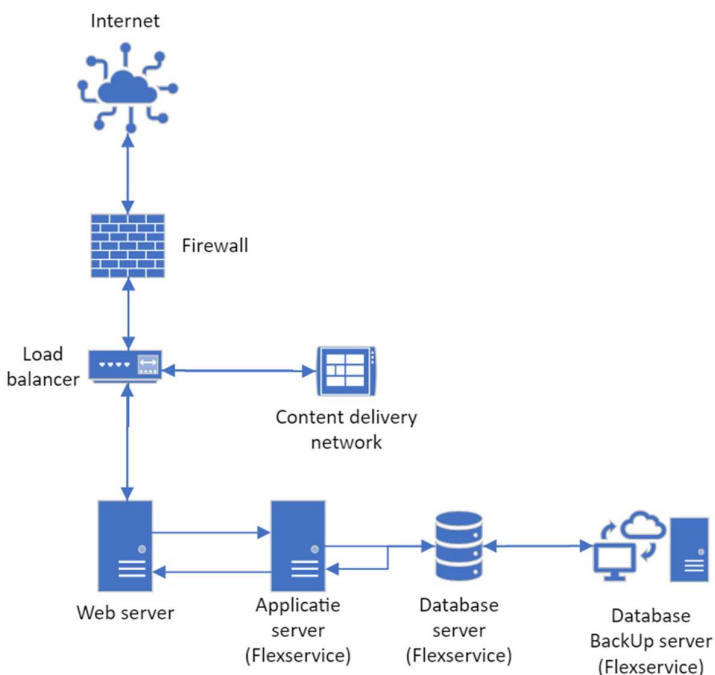
2.2 Gekozen oplossing

IP whitelisting

Om het huidige probleem op te lossen voor Manpower wordt er als oplossing een IP whitelisting systeem gemaakt voor Flexservice. Dit systeem zal toegang tot het Flexservice-platform beperken tot vooraf goedgekeurde IP-adressen. Alleen netwerken die door Manpower als veilig en betrouwbaar worden beschouwd, worden toegelaten. Dit zorgt ervoor dat medewerkers alleen maar vanaf goedgekeurde locaties toegang hebben tot het systeem, wat de veiligheid van gevoelige gegevens aanzienlijk verbetert. De oplossing is relatief goedkoop en het voorkomt verdere aanvallen in onveilige netwerken. Het biedt manpower meer controle over waar en hoe het systeem wordt benaderd.

De reden dat er niet gekozen is voor een VPN verbinding is omdat de oplossing veel geld kan gaan kosten voor Manpower, en het voorkomt niet dat medewerkers gaan werken vanuit netwerken die niet beveiligd zijn. Nadat er al een aanval is geweest vanuit een onbeveiligd netwerk is het vertrouwen in onbeveiligde netwerken laag vanuit medewerkers en uitzendkrachten wiens data nu op straat ligt. Met deze oplossing kan nu alleen nog maar gewerkt worden vanuit vertrouwbare netwerken zoals het thuisnetwerk van een medewerker. Daarmee maakt Manpower een stap naar een Policy waarin werknemers niet meer vanuit onbeveiligde netwerken kunnen werken met Flexservice.

2.3 Netwerk en Systeem diagrammen.



Figuur 1 Webhosting van flexservice van Manpower diagram

In figuur 1 is de huidige situatie van Manpower met het gebruik van Flexservice te zien. Hier zie je dan ook dat werknemers vanaf het internet de webserver van Manpower benaderen en daarbij de applicatie van Flexservice kunnen bereiken.

Internet: Dit het punt waarmee de Gebruikers verbinding maken om toegang te krijgen tot de diensten en inhoud van het netwerk.

Firewall: Dient als de eerste verdedigingslinie tussen het internet en het interne netwerk, filtert inkomende en uitgaande verbindingen voor beveiliging.

Load Balancer: Geplaatst achter de firewall, verdeelt de load balancer het netwerkverkeer gelijkmatig over de web- en applicatieservers om overbelasting te voorkomen en de beschikbaarheid te verhogen.

Content Delivery Network (CDN): Het CDN is verantwoordelijk voor het verspreiden van statische inhoud, zoals afbeeldingen, video's en andere bestanden, over geografisch verspreide servers. Dit vermindert de belasting op de webserver en versnelt de levering van inhoud aan de werknemers.

Webserver: Deze servers hosten de web-interface van Flexservice, die toegankelijk is voor gebruikers nadat ze door de load balancer zijn geleid.

Applicatieserver: : Deze servers draaien de Flexservice applicatie zelf, verwerken de bedrijfslogica en handelen gebruikersacties af. Applicatieservers communiceren rechtstreeks met de database.

Database Server: De centrale opslag voor alle gegevens van Flexservice, inclusief personeelsgegevens, contracten, en andere gevoelige informatie. Deze server staat in directe verbinding met de applicatieservers.

Database Backup Server: Hier worden back-ups van het systeem gemaakt en bewaard voor disaster recovery.

2.4 Kwaliteitscriteria en risicomitigaties.

Bij de implementatie van een IP whitelist systeem voor Manpower is het van groot belang om kwaliteitscriteria vast te stellen die de effectiviteit en betrouwbaarheid van het systeem waarborgen. Het systeem moet niet alleen bescherming bieden tegen ongeautoriseerde toegang maar ook naadloos te integreren zijn met de huidige bedrijfsprocessen van Manpower. Daarnaast is het belangrijk om potentiële risico's te identificeren en maatregelen te treffen om deze te mitigeren

Kwaliteitscriteria:

1. **Nauwkeurige Toegangscontrole:** Het systeem moet accuraat alleen verkeer van geautoriseerde IP-adressen toelaten, waarbij fouten in toegangsbeheer geminimaliseerd worden.
2. **Systeemcompatibiliteit:** De IP whitelist-oplossing moet compatibel zijn met bestaande infrastructuur en software zonder dat dit ten koste gaat van de prestaties.
3. **Flexibiliteit en Schaalbaarheid:** Het systeem moet aanpasbaar zijn om nieuwe vertrouwde IP-adressen op te nemen en moet kunnen opschalen als de organisatie groeit.
4. **Gebruiksvriendelijk Beheer:** Beheerders moeten eenvoudig IP-adressen kunnen toevoegen of verwijderen met een interface.
5. **Audit- en Rapportagecapaciteiten:** Het systeem moet gedetailleerde logs bieden over toegangspogingen en wijzigingen in de whitelist voor compliance doeleinden.
6. **Responsiviteit:** Het systeem moet realtime wijzigingen in de IP-whitelist ondersteunen zonder vertraging in de netwerkprestaties.

7. **Naadloze Integratie:** Het systeem moet compatibel zijn met andere beveiligingsoplossingen zoals firewalls, intrusion detection systemen en security information and event management (SIEM) systemen.

Risicomitigaties:

1. **Regelmatige Updates en Onderhoud:** Om aan te passen aan veranderende netwerkconfiguraties en potentiële beveiligingsdreigingen, moet het systeem regelmatig worden bijgewerkt en onderhouden.
2. **Incident Response Plan:** Een duidelijk plan voor wanneer een ongeautoriseerd toegangspoging wordt gedetecteerd, inclusief snelle isolatie van het betreffende netwerksegment.
3. **Training en Bewustwording:** Medewerkers moeten getraind zijn in het veilig gebruik van het systeem en moeten de beveiligingsprotocollen begrijpen.
4. **Toegangsbewaking:** Continu monitoren van toegangspogingen en onmiddellijke waarschuwingen bij verdachte activiteiten.
5. **Incidentenlogboek en Analyse:** Gedetailleerde logboeken bijhouden voor elke toegangspoging, zowel succesvol als afgewezen, om patronen te identificeren die wijzen op potentiële bedreigingen.
6. **Beleid voor Wijzigingsbeheer:** Duidelijke processen en autorisatie voor het maken van wijzigingen in de whitelist, om onbedoelde toevoegingen of verwijderingen te voorkomen.
7. **Juridische Compliance:** het IP whitelist systeem moet voldoen aan relevante wet- en regelgeving, inclusief gegevensbeschermingswetten zoals de AVG.

3 Proof of Concept

3.1 Gebruikte tools en ontwerp

Om een IP whitelisting systeem te ontwikkelen als beveiligingsoplossing voor het Flexservice-platform van Manpower Nederland, is gekozen voor een webgebaseerde benadering met behulp van het Flask webframework. Flask is gekozen vanwege zijn lichtheid, flexibiliteit en de mogelijkheid om snel veilige webapplicaties te ontwikkelen. De hele webapplicatie is Engels talig gemaakt zodat werknemers die geen Nederlandse achtergrond hebben ook goed overweg kunnen met de webapplicatie. Hieronder wordt het ontwerp en de gebruikte tools voor de ontwikkeling van het systeem uitgelicht.

Gebruikte Tools:

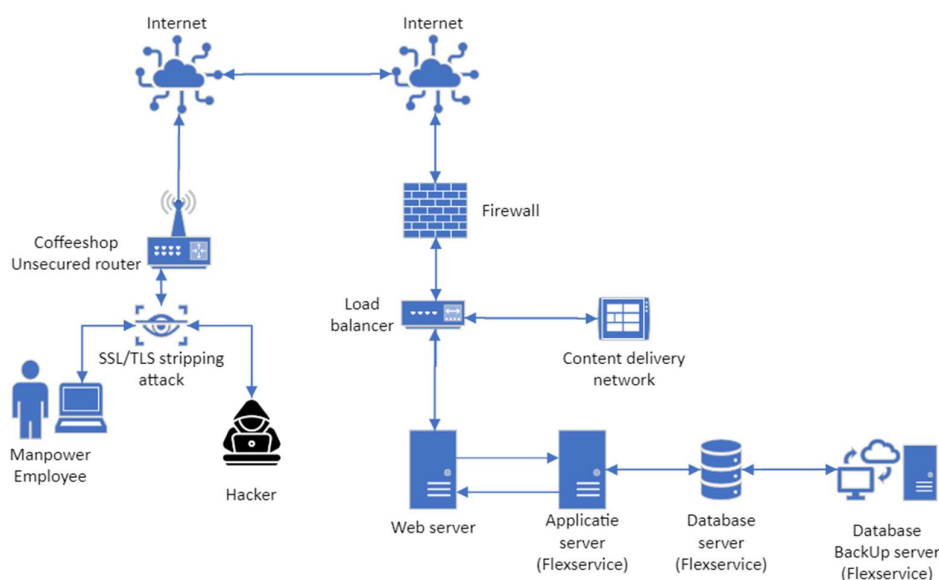
- **Python:** Python is de programmeertaal waarin de flask web toepassing is ontwikkeld. Python wordt gebruik omdat het een relatief makkelijke programmeertaal en omdat het een zeer uitgebreide bibliotheek en modules bevat.
- **Tailwind CSS:** Tailwind CSS is CSS-framework dat wordt gebruikt om de visuele stijl van de web toepassing aan te passen. Met Tailwind is het makkelijk om snel visuele toepassingen door te voeren zonder al te diep in de CSS te duiken
- **HTML:** HTML is gebruikt om de structuur en inhoud van de webpagina's toe te passen. Hiermee werden formulieren voor inloggen en andere pagina-elementen gemaakt en gestructureerd.
- **Flask:** Flask is een webframework voor Python, gekozen voor zijn eenvoudige en lichtgewicht structuur die het snel opzetten van webapplicaties toelaat.
- **MySQL Connector:** Gebruikt om te communiceren met de MySQL-database waarin de IP-whitelist en de gegevens van de admin gebruikers worden opgeslagen.
- **Bcrypt:** Toegepast voor het veilig hashen van wachtwoorden, waardoor een extra beveiligingslaag wordt toegevoegd aan de inlogsystemauthenticatie.
- **Proxy_fix Middleware:** Proxy_fix zorgt ervoor dat de webtoepassing beter begrijpt en correct reageert op informatie die afkomstig is van een proxyserver. Deze code helpt de web toepassing om te weten of er een proxyserver is en wat het originele IP is van de bezoeker.

Ontwerpbeschrijving:

Het IP-whitelist-systeem is opgebouwd uit verschillende delen die elk hun eigen taak hebben:

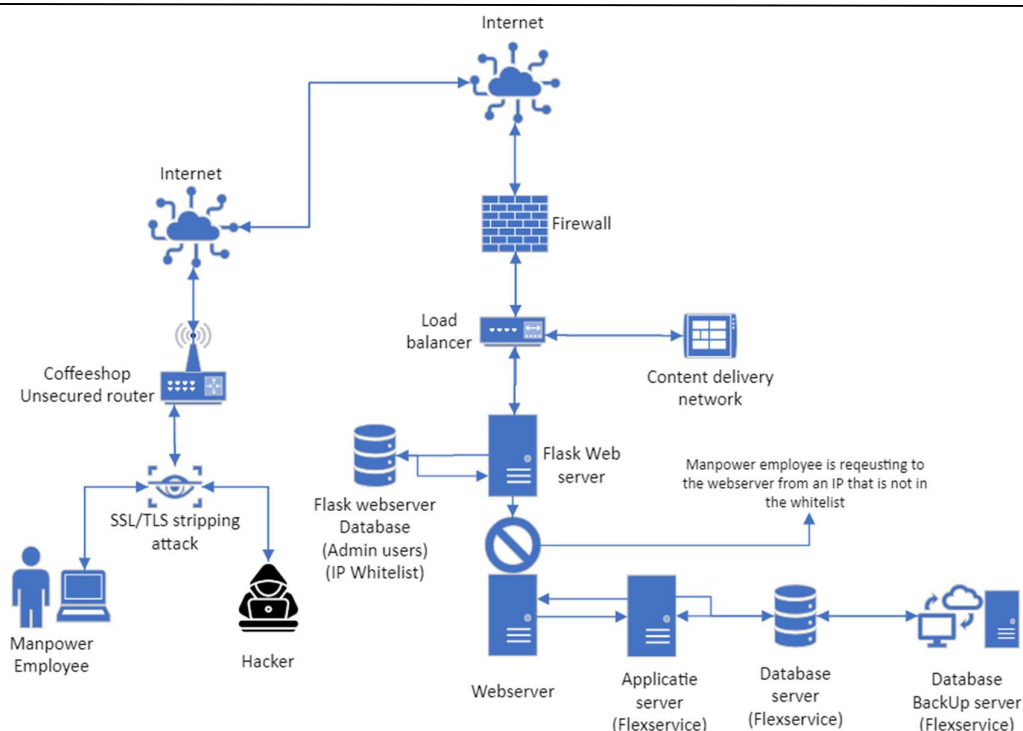
- **Admin Authenticatie:** Hier kunnen beheerders inloggen met hun e-mailadres en wachtwoord, die worden geverifieerd tegen de gehashte gegevens in de database.
- **Whitelist Management Interface:** Een gebruiksvriendelijke interface waarin de admin IP-adressen kan toevoegen, bewerken of verwijderen.
- **Database Design:** De MySQL-database bevat tabellen voor admin gebruikers en IP-whitelist records.
- **IP Whitelist Logica:** Een decoratiefunctie controleert of het IP-adres van een inkomende aanvraag aanwezig is in de whitelist die in de database staat voordat het toegang tot de interface van Flexservice verleend.

3.2 Proces flows, software diagrammen, dialoog diagrammen



Figuur 2 Situatie voor IP Whitelist oplossing

In figuur 2 is te zien hoe de situatie eruit ziet voor Manpower voordat de IP whitelist oplossing is geïmplementeerd. De Manpower medewerker maakt verbinding met de Flexservice webserver vanuit een onbeveiligd netwerk vanuit een café. De medewerker logt in op Flexservice onwetende dat het geen veilige verbinding is en de hacker zijn gegevens ook kan zien.



Figuur 3 Huidige situatie met IP whitelist oplossing

In figuur 3 is de huidige situatie te zien met de IP whitelist oplossing. Omdat het door IP whitelist oplossing niet is toegestaan om vanaf dat IP adres de webserver van Flexservice te benaderen kan de werknemer ook nooit inloggen en zijn gegevens kwijt geven aan de hacker die een SSL/TLS stripping attack uitvoert op de werknemer.

3.3 Gerealiseerde componenten

De IP whitelist oplossing heeft verschillende gerealiseerde componenten ingebouwd. Zo biedt het een admin login waarna de admin na het inloggen op een dashboard komt waar de admin eenvoudig IP adressen van werknemers kan toevoegen, verwijderen of aanpassen in de IP whitelist. De oplossing biedt ook user feedback aan voor de admin bij het inloggen op het inlogschermben en acties die hij uitvoert op het admin panel zoals het toevoegen van IP adressen van werknemers in de IP whitelist. Werknemers die de webserver van Flexservice benaderen vanaf een IP adres die niet in de whitelist staan worden verwezen naar een pagina waar in staat dat ze geen toegang hebben tot Flexservice vanuit hun huidige locatie.

3.4 Testen van Technisch product

Bij het testen van het IP whitelisting systeem voor de toegang tot Flexservice en Manpower, is het belangrijk om zowel de functionaliteit, beveiliging en gebruikersvriendelijkheid te evalueren. Hier zijn een aantal testen om te kijken of het product voldoet:

Functionele Tests

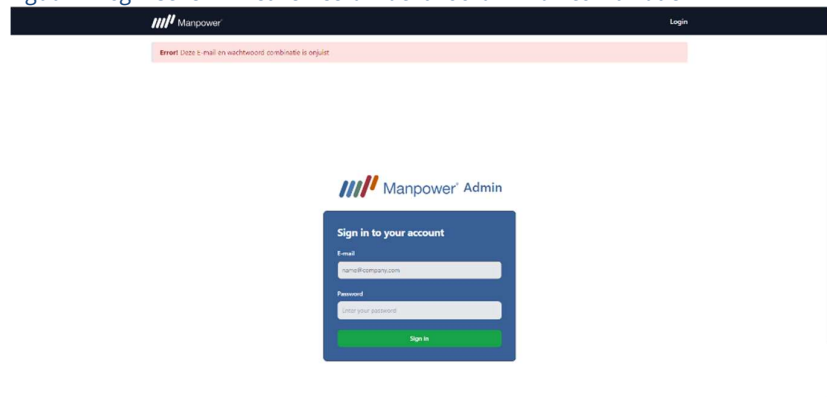
- **Admin authenticatie:** Evalueert het inlogmechanisme door te testen met zowel geldige als ongeldige gebruikersgegevens
- **Whitelist Management:** Evalueert of het systeem correct nieuwe IP-adressen toe kan voegen en kan verwijderen in de whitelist zonder fouten.
- **IP Toegang:** Evalueert of de whitelist functionaliteit goed werkt door zowel met geautoriseerde als niet-geautoriseerde IP-adressen te testen om de nauwkeurigheid van de whitelist functionaliteit te bevestigen.

3.4.1 Testen:

Admin authenticatie test:



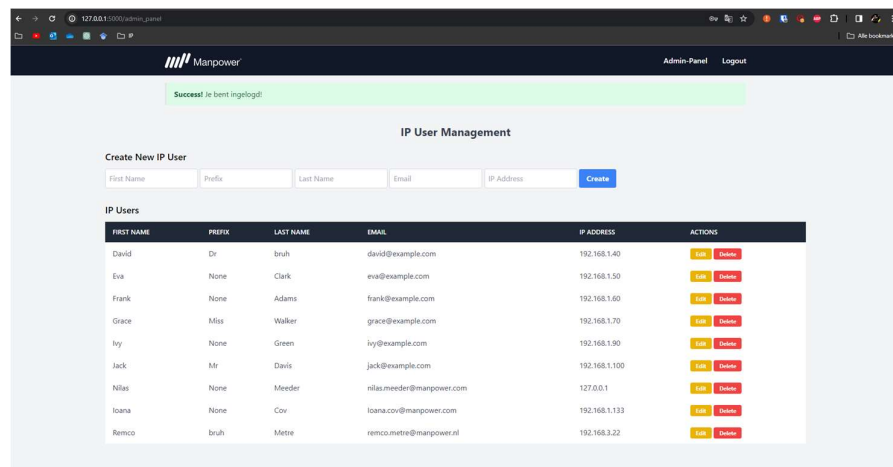
Figuur 4 Login scherm met verkeerd wachtwoord/E-mail combinatie



Figuur 5 Login scherm met melding na verkeerd wachtwoord/E-mail combinatie gebruik

Voor deze test is naar de /admin_login pagina gegaan waarop de admin kan inloggen aan de

hand van het inlog scherm. Als de admin niet is ingelogd en het admin panel probeert te bereiken op de URL /admin_panel dan wordt er geen toegang verleend. Als de admin een verkeerde combinatie van e-mail en wachtwoord intypt met zijn vinger toppen. Dan krijgt de admin een melding op zijn scherm en wordt er nog steeds geen toegang verleend.

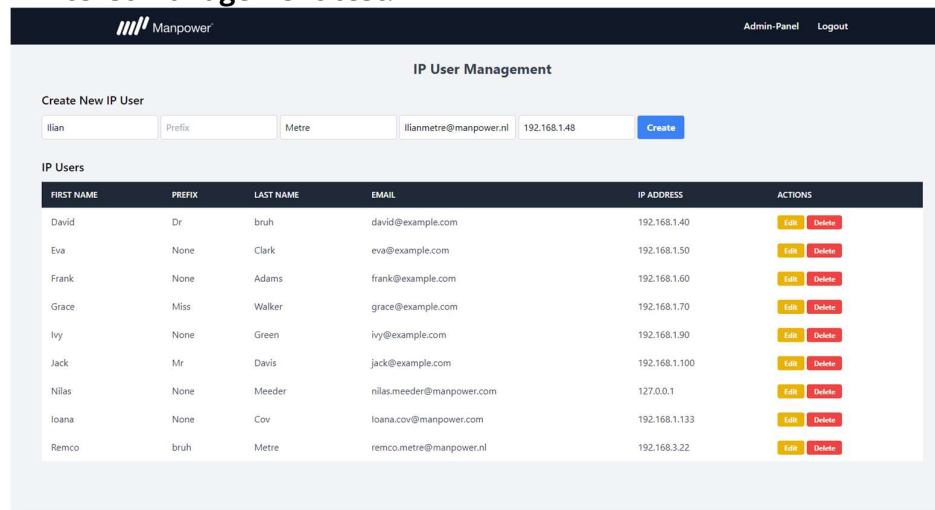


Figuur 6 Admin paneel na inloggen met correcte E-mail en wachtwoord combinatie

Nadat de admin de juiste combinatie met zijn E-mail en wachtwoord heeft ingevoerd op het admin inlog scherm dan beland de admin op het admin paneel met een melding dat hij succesvol is ingelogd zo als te zien is in figuur 6.

Uitkomst: Omdat de admin geen toegang heeft tot het paneel met een fout wachtwoord en E-mail combinatie. Of überhaupt zonder in te loggen kan er wel gezegd worden dat de admin authenticatie tot behoren werkt.

Whitelist Management test:



Figuur 7 Admin paneel met ingevoerde gegevens van een nieuwe gebruiker met IP

In deze test zit de admin op het admin paneel pagina te bereiken bij /admin_paneel na het inloggen. In figuur 7 is te zien Dat admin nieuwe gegevens ingevuld heeft. De gegevens zijn te

zien onder de tekst: "Create new IP user". In dit geval vult de admin De voornaam, achternaam, E-mail, en IP adres in in het formulier.

FIRST NAME	PREFIX	LAST NAME	EMAIL	IP ADDRESS	ACTIONS
David	Dr	bruhr	david@example.com	192.168.1.40	Edit Delete
Eva	None	Clark	eva@example.com	192.168.1.50	Edit Delete
Frank	None	Adams	frank@example.com	192.168.1.60	Edit Delete
Grace	Miss	Walker	grace@example.com	192.168.1.70	Edit Delete
Ivy	None	Green	ivy@example.com	192.168.1.90	Edit Delete
Jack	Mr	Davis	jack@example.com	192.168.1.100	Edit Delete
Nilas	None	Meeder	nilas.meeder@manpower.com	127.0.0.1	Edit Delete
Ioana	None	Cov	ioana.cov@manpower.com	192.168.1.133	Edit Delete
Remco	bruhr	Metre	remco.metre@manpower.nl	192.168.3.22	Edit Delete
Ilian		Metre	ilianmetre@manpower.nl	192.168.1.48	Edit Delete

Figuur 8 Admin paneel na toevoegen van nieuwe gebruiker

Als de admin op het blauwe knopje "Create" drukt die naast het invullen van de gegevens zit wordt een nieuwe gebruiker aan de IP whitelist toegevoegd. In figuur 8 is te zien dat de gebruiker die is ingevuld bij figuur 7 onder aan in het scherm in de lijst staat.

Als de admin een gebruiker wil verwijderen dan hoeft hij simpel enkel op de knop "Delete" te drukken naast de gegevens van de gebruiker die hij wil verwijderen. In deze test is er gekozen om de gebruiker "David DR Bruhr" met het IP adres "192.168.1.40" die in figuur 7 boven aan de lijst staat te verwijderen uit de IP whitelist.

FIRST NAME	PREFIX	LAST NAME	EMAIL	IP ADDRESS	ACTIONS
Eva	None	Clark	eva@example.com	192.168.1.50	Edit Delete
Frank	None	Adams	frank@example.com	192.168.1.60	Edit Delete
Grace	Miss	Walker	grace@example.com	192.168.1.70	Edit Delete
Ivy	None	Green	ivy@example.com	192.168.1.90	Edit Delete
Jack	Mr	Davis	jack@example.com	192.168.1.100	Edit Delete
Nilas	None	Meeder	nilas.meeder@manpower.com	127.0.0.1	Edit Delete
Ioana	None	Cov	ioana.cov@manpower.com	192.168.1.133	Edit Delete
Remco	bruhr	Metre	remco.metre@manpower.nl	192.168.3.22	Edit Delete
Ilian		Metre	ilianmetre@manpower.nl	192.168.1.48	Edit Delete

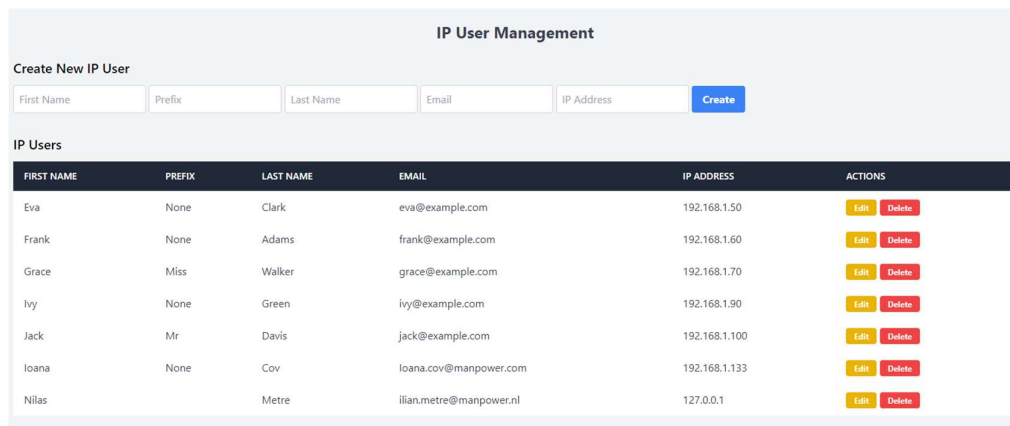
Figuur 9 Admin paneel na verwijderen van gebruiker

In figuur 9 kan je zien dat de gebruiker "David, DR, Bruhr" met het IP adres "192.168.1.40"

verwijderd is uit de IP whitelist.

Uitkomst: De uitkomsten van deze test geven aan dat het management systeem van de IP whitelist voldoet doordat het Gebruikers kan toevoegen en verwijderen uit de lijst.

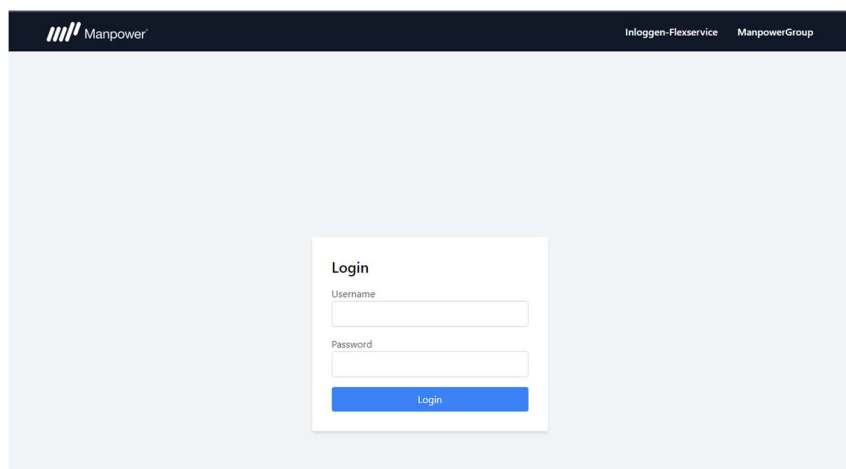
IP Toegang test:



FIRST NAME	PREFIX	LAST NAME	EMAIL	IP ADDRESS	ACTIONS
Eva	None	Clark	eva@example.com	192.168.1.50	Edit Delete
Frank	None	Adams	frank@example.com	192.168.1.60	Edit Delete
Grace	Miss	Walker	grace@example.com	192.168.1.70	Edit Delete
Ivy	None	Green	ivy@example.com	192.168.1.90	Edit Delete
Jack	Mr	Davis	jack@example.com	192.168.1.100	Edit Delete
Ioana	None	Cov	ioana.cov@manpower.com	192.168.1.133	Edit Delete
Nilas		Metre	ilias.metre@manpower.nl	127.0.0.1	Edit Delete

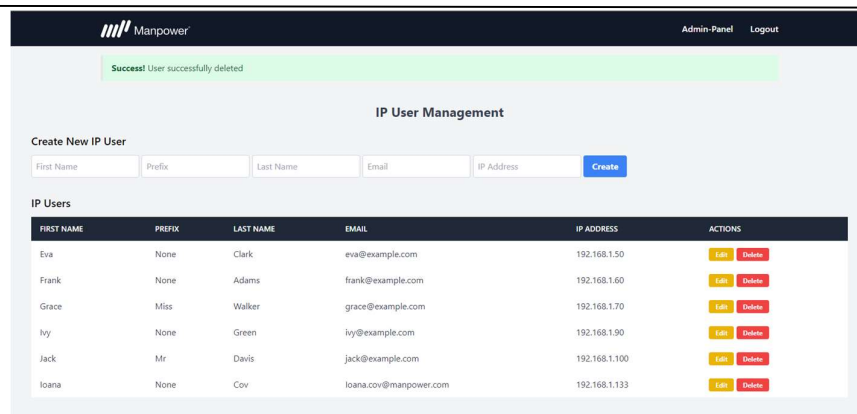
Figuur 10 Admin panel met gebruikers die toegang tot Flexservice hebben

In figuur 10 is onderaan de gebruiker “Nilas Metre” met het IP adres “127.0.0.1” te zien. Deze gebruiker heeft toegang tot de pagina van Flexservice omdat hij in de whitelist staat.



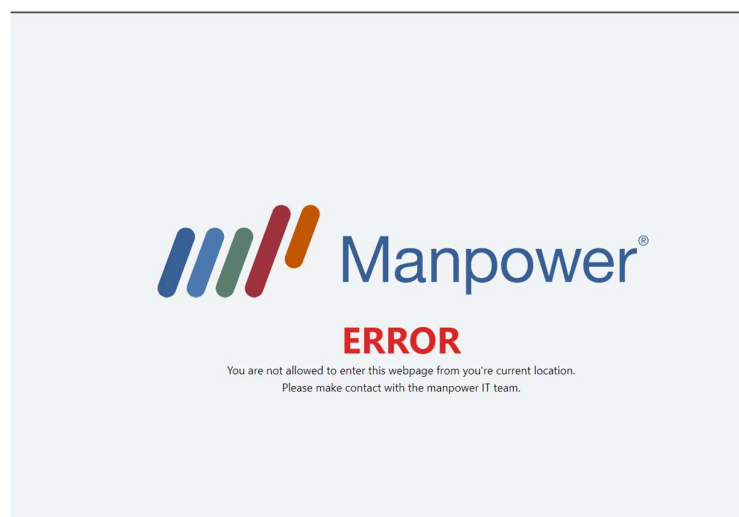
Figuur 11 Inlogscherm Flexservice met een benadering met een IP die in de IP whitelist staat

Als deze gebruiker naar de URL / gaat krijgt hij het inlog scherm van Flexservice aangeboden zoals te zien is in Figuur 11.



Figuur 12 Admin paneel na verwijderen van de onderste gebruiker

In Figuur 11 is te zien dat de gebruiker "Nilas Metre" met het IP adres "127.0.0.1" is verwijderd uit de IP whitelist omdat hij niet meer onder aan de lijst staat.



Figuur 13 Error scherm na het benaderen met een IP die niet in de IP whitelist staat

In Figuur 13 is het error scherm te zien nadat de gebruiker "Nilas Metre" met het IP adres "127.0.0.1" de URL / probeert te benaderen met zijn IP die nu niet meer in de IP Whitelist staat. De gebruiker wordt doorgestuurd naar de URL /error en krijgt geen toegang tot het inlog scherm van Flexservice.

Uitkomst: De uitkomst van deze test voldoet. Als de gebruiker met een IP adres die niet in de IP whitelist staat het Flexservice Inlogschermbenaderd dan heeft hij daar geen toegang tot. Als de gebruiker wel met een IP adres die in de IP whitelist staat dan krijgt de gebruiker wel toegang tot het inlogschermbenaderd van Flexservice.

3.5 Proof of Context conclusie.

De ontwikkeling en implementatie van het IP whitelisting systeem voor Flexservice van Manpower laat het belang zien van het creëren van een effectieve, gebruiksvriendelijke en veilige oplossing om de toegang tot cruciale bedrijfssystemen te beheren zoals Flexservice.

De testresultaten tonen aan dat het systeem effectief is in het beheren van toegang via IP-adressen. Het admin authenticatiemechanisme zorgt ervoor dat alleen geautoriseerde gebruikers wijzigingen kunnen aanbrengen in de IP whitelist. De IP whitelist management interface maakt het eenvoudig voor beheerders om IP-adressen toe te voegen, te verwijderen en te bewerken, wat de werkzaamheden aanzienlijk efficiënter maakt.

De belangrijkste realisatie van dit project is de demonstratie van de veiligheid van Flexservice tegen ongeautoriseerde toegang. Het systeem blokkeert consequent toegangspogingen van IP-adressen die niet op de whitelist staan, waardoor de risico's van cyberaanvallen zoals SSL/TLS stripping in een onbeveiligd netwerk worden verkleint. Dit wordt aangetoond door de positieve en negatieve tests in hoofdstuk 3.4.1, waarbij toegang alleen wordt verleend aan geautoriseerde IP-adressen.

Verder heeft de gebruikersinterface zich bewezen als makkelijk en toegankelijk. Beheerders kunnen gemakkelijk navigeren door het systeem, wat bijdraagt aan een positieve gebruikerservaring.

De proof of concept van het IP whitelist systeem heeft aangetoond dat het een waardevolle toevoeging is aan de beveiligingsinfrastructuur van Manpower. Desondanks dat het een waardevolle toevoeging is aan de beveiligingsinfrastructuur van Manpower mist het nog wel enkele veiligheid functies. Het IP whitelist systeem dat nu gemaakt is voor Manpower vormt wel een goede basis om verder te ontwikkelen met daarbij de veiligheid en betrouwbaarheid van het systeem te verhogen.

4 Eindconclusie

4.1 Conclusie

De implementatie van het IP whitelist systeem voor Flexservice bij Manpower markeert een belangrijke stap in de bescherming tegen de complexe uitdagingen van datalekken in een steeds meer gedigitaliseerde werkomgeving. Dit systeem adresseert specifiek de risico's verbonden aan werknemers die vanuit onveilige netwerken te werk gaan en onvoldoende toegangscontrole van uit systemen - twee primaire factoren die bijdragen aan het verhoogde risico op datalekken in de huidige tijd.

In het licht van de problematiek rond datalekken, zoals geïdentificeerd in het begin van dit project, biedt de ontwikkeling van dit IP whitelist systeem een concrete oplossing om de vertrouwelijkheid, integriteit en beschikbaarheid van gevoelige bedrijfsgegevens te beschermen. Het systeem biedt een verdediging tegen methoden zoals SSL/TLS stripping, waarmee hackers voorheen toegang konden krijgen tot gevoelige informatie van de

medewerkers die vanuit onveilige netwerken te werk gaan.

De functionele en prestatietests hebben de betrouwbaarheid en efficiëntie van het systeem gedemonstreerd, terwijl de gebruikersinterface de administratieve processen voor beheerders vereenvoudigt is. Door het versterken van netwerkbeveiliging en het verbeteren van zwakheden in Flexservice, biedt dit systeem Manpower een solide basis voor het vergroten van betrouwbaarheid en veiligheid binnen de organisatie.

4.2 Advies en aanbevelingen.

Om de veiligheid en betrouwbaarheid van de oplossing te vergroten zijn er een paar punten die Manpower kan meenemen voor toekomst van dit IP whitelist systeem.

1. **Multifactor Authenticatie (MFA):** Om de veiligheid te vergroten en de kans te verkleinen dat er ongeautoriseerde toegang tot het systeem Flexservice is kan Manpower een MFA functie implementeren voor zowel de Admin login tot het IP whitelist systeem en de Flexservice applicatie zelf.
2. **Logstelsysteem:** Manpower kan een gedetailleerd logstelsysteem implementeren voor alle activiteiten gerelateerd aan de IP whitelist. Het logstelsysteem zou waardevolle inzichten bieden in toegangspatronen en potentiële beveiligingsincidenten. Dit systeem zou zowel succesvolle als mislukte toegangspogingen moeten registreren, maar ook wijzigingen in de IP whitelist.
3. **Automatisering:** Manpower kan een geautomatiseerd systeem maken voor het toevoegen van IP-adressen aan de IP whitelist. Het maken van dit systeem kan ervoor zorgen dat menselijke fouten worden verminderd bij het toevoegen van IP adressen aan de IP whitelist.
4. **Regelmatige Beveiligingsaudits en -beoordelingen:** Het is vooral aangeraden om regelmatig beveiligingsaudits uit om kwetsbaarheden in het systeem te identificeren en aan te pakken. Dit zou moeten helpen bij het handhaven van de hoogste beveiligingsstandaarden en bij het tijdig aanpakken van nieuwe dreigingen.
5. **Incidentresponsplan:** Het is ook met groots aan te raden dat Manpower een gedetailleerd incidentresponsplan opstelt dat specifiek gericht is op mogelijke datalekken en beveiligingsincidenten die met dit systeem te maken hebben. Dit plan moet procedures bevatten voor onmiddellijke actie, communicatie en herstel in het geval van een beveiligingsinbreuk.

5 Verwijzingen

- AP. (z.d). *Datalek? Dit moet u doen*. Opgehaald van autoriteitpersoonsgegevens.nl:
<https://www.autoriteitpersoonsgegevens.nl/themas/beveiliging/datalekken/datalek-dit-moet-u-doen>
- AP. (z.d). *Wat is een datalek?* Opgehaald van autoriteitpersoonsgegevens.nl:
<https://www.autoriteitpersoonsgegevens.nl/themas/beveiliging/datalekken/wat-is-een-datalek>
- Gitlan, D. (2023, December 21). *What Is an SSL Stripping Attack and How to Prevent It*. Opgehaald van ssldragon.com: <https://www.ssldragon.com/blog/ssl-stripping/>
- Kaspersky. (z.d). *Hoe vermijd ik de beveiligingsrisico's van openbare wifi?* Opgehaald van kaspersky.nl: <https://www.kaspersky.nl/resource-center/preemptive-safety/public-wifi-risks>
- KVK. (2021, september 16). *Zo voorkom je een datalek*. Opgehaald van kvk.nl:
<https://www.kvk.nl/veilig-zakendoen/zo-voorkom-je-een-datalek/>
- Manpower. (z.d). *Ons bedrijf*. Opgehaald van manpower.nl: <https://www.manpower.nl/nl/over-manpower/ons-bedrijf>
- manpowergroup. (z.d). *Onze Merken*. Opgehaald van manpowergroup.nl:
<https://manpowergroup.nl/onze-merken/>
- Martijn Broekhof, J. (2023, Januari 21). *MELDPLICHT DATALEKKEN: HOE KAN EEN ACCOUNTANT HAAR CLIËNTEN HELPEN?* Opgehaald van guardian360.nl:
<https://www.guardian360.nl/meldplicht-datalekken-hoe-kan-een-accountant-haar-clienten-helpen/>
- Murat, O., Kose, Y., Bastug, M. F., & Kucukkaya, G. (2023, November 30). *The Shifting Landscape of Cybersecurity: The Impact of Remote Work and COVID-19 on Data breach trends*. Opgehaald van researchsquare: <https://assets.researchsquare.com/files/rs-3630534/v1/2d48f97d-165f-4aa7-87f3-17ad0c6d2605.pdf?c=1702669945>
- OldNational. (2019, October 7). *Examining the Financial Consequences of a Data Breach*. Opgehaald van oldnational.com:
<https://www.oldnational.com/resources/insights/examining-the-financial-consequences-of-a-data-breach/>
- PayPal. (2023, December 14). *Long-term consequences of a data breach: Prevention strategies and recovery roadmap creation*. Opgehaald van paypal.com:
<https://www.paypal.com/us/brc/article/consequences-of-data-breach>
- Peeters, W. (2018). *Van leerdoelen naar leeruitkomsten*. Opgehaald van Vernieuwonderwijs:
<https://www.vernieuwonderwijs.nl/van-leerdoelen-naar-leeruitkomsten/>
- R, B., & E. A., A. M. (2017, April 20). *A survey on data breach challenges in cloud computing security: Issues and threats*. Opgehaald van ieeexplore.ieee.org:
<https://ieeexplore.ieee.org/abstract/document/8074287>
- TNO. (2023, Oktober 26). *Aantal thuiswerkuren sinds coronapandemie fors gestegen*. Opgehaald van tno.nl: <https://www.tno.nl/nl/newsroom/2023/10/corona-thuiswerkuren-gestegen/>
- Vanmorgen, Accountancy. (2023, Februari 22). *Vermeend datalek bij Manpower is Deloitte-accountants niet aan te rekenen*. Opgehaald van accountancyvanmorgen.nl:
<https://www.accountancyvanmorgen.nl/2023/02/22/vermeend-datalek-bij-manpower->

is-deloitte-accountants-niet-aan-te-rekenen/
VDB Advocaten Notarissen. (2021, Januari 27). *Datalekken & de AVG*. Opgehaald van vdb-law.nl:
<https://vdb-law.nl/nieuws/datalekken-de-avg>

Bijlage A, Logboek en reflectie

Logboek

Datum	Uren besteed	Activiteit
5 December	0.5	Problematiek kiezen
13 December	1	Problematiek uitzoeken – Wat is datalekken door werken op afstand precies?
18 December	2	Context creëren. Online gekeken naar realistische contexten die ik kan gebruiken.
20 December	1.5	Poster maken
21 December	1	Poster presentatie
11 Januari	4	Andere context gekozen door implicaties
13 Januari	2	Uitzoeken Mogelijke oplossingen
15 Januari	5	Realistische context gevonden. Scope opnieuw aangepast zodat het beter bij de context valt
17 Januari	6	Gekozen aanpak, Security aspecten en kwaliteits criteria
18 Januari	6	Mogelijke oplossingen, gekozen oplossing, Netwerk en systeem diagrammen
19 Januari	8	Kwaliteitscriteria en risicomitigaties en Product bezig geweest
20 Januari	10	Product afgemaakt. Gebruikte tools en ontwerp, Proces flows software diagrammen. Geraliseerde componenten.
21 Januari	9	Testen, Proof of context conclusie, Eindconclusie en reflectie.

Reflectie

Ik vond het een lastig project omdat er veel documentatie aan vast voor het IP en het TP. Eerst keek ik hier heel erg tegen op en dit belemmerde ook heel erg mijn motivatie voor het maken van dit project. Daardoor was mijn tijd planning heel slecht en heb ik relatief weinig uitgevoerd de eerste weken van blok 2. Was de deadline niet verschoven dan had ik het ook niet gehaald. (Dank aan de docenten om ons deze speling te geven).

Het moeilijkste van dit project vond ik de problematiek en context juist krijgen. Ik heb hier dan ook heel lang over lopen piekeren omdat het voor mijn gevoel niet helemaal klopte. Daarna vond ik de juiste oplossing kiezen ook heel moeilijk. Voor de hand liggend was een VPN maken maar dat heb ik al met TP1 gemaakt. Toch ben ik uiteindelijk blij met mijn werk. Ik vindt dat ik goede bronnen heb en vind dat ik uiteindelijk een best mooi product heb kunnen maken die aan mijn verwachtingen voldoen. IP1 is met dit verre van te vergelijken. Ik heb vooral de laatste week heel hard aan dit project gewerkt en ik hoop dat dan ook met een voldoende voor het IP af te sluiten.

Wat ik leuk vind aan het IP1 is dat ik nu zelf helemaal het technische gedeelte moet doen. Het is mij nog nooit helemaal gelukt om in mijn eentje een Flask omgeving op te zetten. Tuurlijk hebben wij dit gedaan in recente projecten maar daar ben ik vooral bezig geweest met de front-end en een gedeelte van de backend. Nu heb ik helemaal zelf de website laten werken en het heeft mij veel technische kennis gegevens over Python en Flask.

Het grootste obstakel waar ik technisch tegen aanliep was het correct identificeren van de IP adressen van degene die de webpagina opvragen. Ook om het hele admin panel te laten werken ben ik veel tijd aan kwijt geraakt. Gelukkig werkt alles uiteindelijk.

Ik neem mee uit dit project hoe belangrijk het is om te weten wat de organisatie allemaal doet, hoe de organisatie precies in elkaar zit en hoe je over alles moet nadenken voordat je een oplossing voor een probleem gaat maken.

Bijlage B, optioneel

Bijvoorbeeld: Detailtekeningen, tests, filmpjes of plaatjes (bewijs), code

```
# Function to check if an IP address is whitelisted
def ip_whitelist(ip_address):
    # Connect to the database
    connect = mysql.connector.connect(**config)
    cursor = connect.cursor()

    try:
        # SQL query to count IP address in the database
        query = "SELECT COUNT(1) FROM fs_users WHERE ip_addr = %s;"
        cursor.execute(query, (ip_address,))

        # Fetch the result which is a tuple
        result = cursor.fetchone()

        # Check if the count is more than 0, if more than 1 IP address is
        # whitelisted
        return result[0] > 0

    # Handle any exceptions with the MySQL database such as connection issues or SQL
    # error
    except mysql.connector.Error as err:
        print(f"Error: {err}")

        # Return False to show that the IP address is not whitelisted because of
        # the error
        return False

    # Close the cursor and the database connection
    finally:
        cursor.close()
        connect.close()

# Function to get the client's IP address from the request
def get_client_ip(request):
    ip = request.remote_addr
    return ip

# Decorator function to check if the client's IP is whitelisted
def check_ip(func):
    @wraps(func)
    def decorated_function(*args, **kwargs):
        visitor_ip = get_client_ip(request)
        if not ip_whitelist(visitor_ip):
            return redirect(url_for('auth.location_error'))
```

```
        return func(*args, **kwargs)
    return decorated_function

# Route for the home page, with IP whitelist check
@auth.route('/')
@check_ip
def home():
    return render_template('Flexservice.html')

# Route for displaying a location error page when ip is not in whitelist
@auth.route('/error')
def location_error():
    return render_template('location_error.html')
```