4-7-2025

Functioneel ontwerp

Vlammend Varken

Noureddin Alkeswani, Bradley Malasch, Michel Knols

NBM Solutions V1.0

Inhoud

[Inleiding 2](#_Toc202285078)

[Opdrachtgever 2](#_Toc202285079)

[Doelgroepen 2](#_Toc202285080)

[Doelstelling 2](#_Toc202285081)

[Randvoorwaarden 3](#_Toc202285082)

[Uitgangspunten 3](#_Toc202285083)

[Gap-analyse 4](#_Toc202285084)

[Analysefase 4](#_Toc202285085)

[Problemen en requirements 5](#_Toc202285086)

[Prioriteringstechniek 5](#_Toc202285087)

[Requirements 6](#_Toc202285088)

[Azure Architectuur 7](#_Toc202285089)

[Azure Cloud 7](#_Toc202285090)

[Servers 7](#_Toc202285091)

[Virtual Machines (VM’s) 8](#_Toc202285092)

[Netwerkverbindingen 8](#_Toc202285093)

[Lokale computers en Tablets 8](#_Toc202285094)

[API Management (APIM) 8](#_Toc202285095)

[Beveiliging 9](#_Toc202285096)

[Multifactor Authentication (MFA) 9](#_Toc202285097)

[Enterprise User Management 9](#_Toc202285098)

[Microsoft Entra ID 9](#_Toc202285099)

[Network Security Group (NSG) 10](#_Toc202285100)

[Azure Firewall 10](#_Toc202285101)

[Back-up & Recovery 10](#_Toc202285102)

[Logging 10](#_Toc202285103)

[Private Endpoint Connection(s) 10](#_Toc202285104)

[VPN Gateway 11](#_Toc202285105)

[Proof of Concept (POC) 11](#_Toc202285106)

[Gerealiseerde onderdelen 11](#_Toc202285107)

[Beperkingen 11](#_Toc202285108)

[Bibliografie 12](#_Toc202285109)

# Inleiding

Dit document beschrijft op hoofdlijnen de eisen en wensen van Vlammend Varken met betrekking tot een digitale infrastructuur en een geïntegreerd digitaal systeem. Deze wensen en eisen zijn vertaald naar concrete randvoorwaarden en requirements. Op basis hiervan is een concept opgesteld met de benodigde services, gebruikersrollen en componenten.

Het ontwerp richt zich onder andere op het opzetten van een digitale bestelomgeving, waarbij veilig ingelogd moet kunnen worden. Er wordt gebruik gemaakt van Virtual Machines (VM’s) op Microsoft Azure en een versleutelde webomgeving via HTTPS.

Wanneer de opdrachtgever akkoord gaat met dit functioneel ontwerp (FO), zal dit document dienen als blauwdruk voor het technisch ontwerp (TO).

# Opdrachtgever

De opdrachtgever voor deze casus is dhr. Bekker, eigenaar van restaurant Vlammend Varken.

# Doelgroepen

De volgende doelgroepen vallen binnen de scope van dit project:

* De gasten;
* De eigenaar;
* De medewerkers (obers, chef-koks)

De doelgroep *Leveranciers* valt op dit moment buiten de scope.

# Doelstelling

Vlammend varken is momenteel bezig met een renovatie en wil tegelijkertijd de digitale infrastructuur vernieuwen. Het doel is om een geïntegreerd digitaal systeem te laten ontwikkelen dat de bedrijfsvoering toekomstbestendig maakt en aansluit bij de duurzame missie van het restaurant.

De kernprocessen die gedigitaliseerd moeten worden, zijn als volgt:

* Gasten kunnen via een tablet aan tafel gerechten bekijken, aanpassen en direct bestellen.
* Chef-koks krijgen een overzicht van binnengekomen bestellingen en kunnen deze efficiënt afhandelen.
* Chef-koks moeten dagelijks een menu kunnen samenstellen op basis van actuele voorraad en verwachte leveringen.
* Het systeem bevat standaardmodules zoals een reserveringssysteem, betaalfunctionaliteit en voorraadbeheer.

# Randvoorwaarden

1. De digitale infrastructuur wordt ingericht in de cloud.
2. Op locatie wordt gewerkt met tablets; gasten plaatsen bestellingen via deze tablets aan tafel.
3. Een gast moet in maximaal twee stappen een bestelling kunnen plaatsen.
4. Het systeem moet eenvoudig te gebruiken zijn medewerkers en vereist geen aparte training.
5. De scope van dit project is beperkt tot het bestelproces.

# Uitgangspunten

1. Gebruikersgroepen: Gebruikers dienen vaardig te zijn in het gebruik van een tablet.
2. Toegangsbeleid: Medewerkers loggen in via Entra ID en maken gebruik van multifactor authenticatie (MFA).
3. Omgeving: De digitale omgeving is cloudgebaseerd en wordt niet lokaal (on-premise) ingericht.
4. Beschikbare middelen: Er wordt gewerkt met tablets en een lokale pc.
5. Beveiligingseisen: Al het verkeer tussen client en de WebApp-server verloopt via HTTPS. De API-VM en de achterliggende SQL Server zijn alleen via private netwerken toegankelijk. Alleen de beheerder heeft toegang via een aparte beheerder-VM.
6. Technische scope: Er wordt gebruikgemaakt van een eigen domein met uitsluitend intern bereikbare adressen.

# Gap-analyse

**Huidige situatie**

Er is op dit moment geen digitale infrastructuur aanwezig; deze moet volledig worden ingericht. Gasten ervaren lange wachttijden voordat een ober hun bestelling kan opnemen. Bestellingen en reserveringen worden handmatig verwerkt, wat leidt tot fouten en inefficiënte. Daarnaast missen medewerkers overzicht in zowel bestellingen als voorraden.

**Gewenste situatie**

Vlammend Varken streeft naar een digitale infrastructuur die eenvoudig en veilig is in gebruik, zowel voor gasten als medewerkers. Er is gekozen voor een implementatie binnen Microsoft Azure. Hiervoor worden meerdere VM’s ingericht, waaronder een voor de beheerder, de API, de SQL Server en de WebApp-server. Via een beveiligde verbinding met de WebApp-server kunnen menu’s zowel thuis als op locatie worden bekeken. Bestellingen kunnen uitsluitend op locatie worden geplaatst via de aanwezige tablets.

## Analysefase

Uit het gesprek met de opdrachtgever is gebleken dat het huidige proces rondom bestellingen, voorraadbeheer en algemeen management moeizaam verloopt. Vooral het wijzigen van gerechten kost veel tijd, doordat alle nog handmatig gebeurt. Dit maakt het proces foutgevoelig en inefficiënt.

De opdrachtgever wil een systeem dat eenvoudig in gebruik eenvoudig is voor zowel gasten als medewerkers. Daarnaast moet het systeem inzicht bieden in de bedrijfsvoering, waaronder bestellingen, reserveringen, voorraden en de inzet van medewerkers. In overleg is afgesproken dat de scope zich in deze fase beperkt tot het onderdeel bestellingen.

Er is expliciet gekozen om geen lokale serverinfrastructuur op te zetten; enkel de bestaande lokale internetinfrastructuur wordt gebruikt. Hoewel het oorspronkelijke casusdocument aangaf dat gasten via hun telefoon moesten kunnen bestellen, is dit tijdens het gesprek met de opdrachtgever bijgesteld: er zal uitsluitend gebruik worden gemaakt van tablets op locatie.

naar voren gekomen dat het huidige proces van bestellen, voorraadbeheer en management in het algemeen moeizaam verloopt. De wijzigingen van de gerechten kost het meeste tijd. Dit komt omdat nog alles met de hand gedaan wordt en dit een grote foutgevoeligheid introduceert.

## Problemen en requirements

De opdrachtgever heeft de volgende aanvullende eisen voor het ontwerp geformuleerd:

* Gasten plaatsen hun bestellingen zelf via een tablet.
* Gasten moeten binnen twee stappen een bestelling kunnen plaatsen.
* Wanneer tafels worden samengevoegd, wordt het laagste tafelnummer gebruikt als koppelnummer voor de bestelling.
* Medewerkers moeten het systeem kunnen gebruiken zonder training.
* Zodra een chef-kok begonnen is met de voorbereiding, kan een bestelling niet meer worden gewijzigd.
* De chef-kok is verantwoordelijk voor de samenstelling van gerechten.
* De chef-kok beheert de voorraad van de ingrediënten.
* Obers beheren de drankenkaart.

De eisen zijn grofweg te clusteren in drie categorieën:

* Gebruikersgemak (User Interface)
* Bestellogica (API/Backend)
* Beheerfuncties (rollen en rechten)

Sommige functies zijn afhankelijk van een correcte roltoekenning en toegangscontrole. Zo mag alleen de kok toegang hebben tot voorraadbeheer.

## Prioriteringstechniek

Voor het prioriteren van de requirements is gekozen voor de methode *Requirements Triage*. Hierbij worden eisen ingedeeld op basis van hun noodzaak binnen de scope van het systeemonderdeel bestellingen. De indeling bestaat uit drie categorieën:

* Must: essentieel voor correcte werking van het systeem
* Should: belangrijk, maar niet kritisch
* Could: optioneel, verhoogd gebruiksvriendelijk of flexibiliteit

De indeling is gemaakt op basis van het belang voor de eindgebruiker (zoals beschreven in de userstories), het effect op het systeemgedrag en afhankelijkheden binnen de infrastructuur.

# Requirements

Onderstaand overzicht bevat de functionele en niet-functionele requirements die zijn afgeleid uit de gesprekken met de opdrachtgever en de analysefase. Elke requirement is voorzien van een unieke code, een bijbehorende userstory, een korte omschrijving, het type requirement, de actor, en een prioriteit van de Requirements Triage-methode (Should, Could, Must). Dit overzicht dient als leidraad voor de verdere uitwerking van het technisch ontwerp en vormt tevens de basis voor ontwerpbeslissingen en validatie in latere projectfasen.



# Azure Architectuur

Onderstaande *Figuur 1— (Azure Infrastructuur)* geeft een visuele weergave van de voorgestelde infrastructuur binnen Microsoft Azure. Deze architectuur vormt de technische basis voor het systeem dat Vlammend Varken ondersteunt bij het digitaal verwerken van bestellingen.

De infrastructuur omvat verschillende VM’s en platformdiensten, waaronder de webapplicatie, API-server, SQL-server en de beheeromgeving. Elke component heeft een specifieke rol, wat resulteert in een veilige, schaalbare en gestructureerde opzet.

Afbeelding met tekst, schermopname, diagram, Perceel

Door AI gegenereerde inhoud is mogelijk onjuist.

Figuur : Azure Infrastructuur.

## Azure Cloud

Azure is het cloudplatform van Microsoft waarin VM’s en diverse diensten worden gehost. Vlammend Varken maakt gebruik van deze omgeving om een webserver, een SQL-server en een werkomgeving voor medewerkers en beheerders veilig in te richten.

## Servers

Binnen de Azure-omgeving draaien verschillende virtuele servers, waaronder de webserver waarop medewerkers via een browser kunnen inloggen. Voor de inrichting van de SQL-server en de webapplicatieserver is gekozen voor een Platform as a Service (PaaS)-oplossing. Dit betekend dat alle resource-instellingen binnen Azure worden beheerd door Microsoft, met uitzonering van de data en de applicatie zelf. De beheerder- en API-VM zijn wél volledig handmatig samengesteld, zodat er meer controle is over de gebruikte resources.

## Virtual Machines (VM’s)

Een VM is een virtuele computer die wordt gehost binnen de Azure-cloud. Elke medewerker of beheerder krijgt via de API-VM toegang tot de SQL-server en de bijbehorende database.

## Netwerkverbindingen

De netwerkcomponenten op de locatie van Vlammend Varken, zoals routers, switches en servers, zijn via ethernetkabels met elkaar verbonden. Dit zorgt voor een stabiele en snelle netwerkverbinding. De tablets die door gasten en medewerkers worden gebruikt, maken draadloos verbinding via wifi.

## Lokale computers en Tablets

De lokale apparaten, waaronder pc’s en tablets, worden gebruikt door de eigenaar en medewerkers. Via een actieve netwerkverbinding loggen zij veilig in op de SQL-server in de Azure-omgeving. Dankzij MFA zijn de verbindingen extra beveiligd. De tablets draaien op Android en worden zodanig ingericht dat medewerkers uitsluitend toegang hebben tot de functies waarvoor zij gemachtigd zijn.

## API Management (APIM)

De API Management-service van Azure wordt ingezet om de toegang tot de API te beheren. Deze service beheert verbindingen, registreert activiteiten en logt gebruik. APIM is géén beveiligingslaag, maar puur een beheermodule. In de infrastructuur van Vlammend Varken verzorgt de APIM de communicatie tussen de webapplicatieserver en de API-VM. Hierbij ontvangt de webapp via Entra ID de juiste rol en token, die vervolgens wordt doorgestuurd naar de API-VM. Deze haalt op basis van die rechten de relevante data op uit de SQL-server.

# Beveiliging

Voor de digitale infrastructuur van Vlammend Varken zijn verschillende beveiligingsmaatregelen getroffen op de vertrouwelijkheid, integriteit en beschikbaarheid van gegevens te waarborgen. De beveiliging is ingericht op meerdere niveaus: authenticatie, toegangsbeheer, netwerkbescherming, logging en herstel bij incidenten. Onderstaand worden de belangrijkste componenten toegelicht.

Multifactor Authentication (MFA)  
Voor het inloggen op de SQL-server maakt Vlammend Varken gebruik van multifactor authenticatie. Gebruikers moeten na het invoeren van hun wachtwoord een extra verificatiestap doorlopen via de Microsoft Authenticator-app. Bij een inlogpoging ontvangt de medewerker een melding op zijn telefoon om de login te bevestigen of een eenmalige code in te voeren. Toegang wordt alleen verleend wanneer beide verificatiefactoren kloppen en de gebruiker tot de juiste groep behoort.

## Enterprise User Management

Binnen de Azure-omgeving wordt Enterprise User Management ingezet voor het beheer van gebruikersgroepen en toegangsrechten. Zo hebben verschillende rollen, zoals directeur of administratief medewerker, elk hun eigen rechtenniveau. Het systeem zorgt ervoor dat accounts gekoppeld kunnen worden aan de juiste groepen met de bijbehorende toegangsrechten. (Microsoft, 2025b)

Dit is het systeem binnen Azure dat gebruikersgroepen beheert en de toegangsrechten. Zo heeft een directeur andere rechten dan een administratief medewerker. Dit systeem zorgt ervoor dat een account aan de juiste groep gekoppeld is met de bijbehorende rechten

Microsoft Entra ID

Microsoft Entra ID is de identiteits- en toegangsbeheeroplossing van Microsoft. Hiermee wordt geregeld dat alleen geautoriseerde gebruikers toegang krijgen tot bepaalde onderdelen van het systeem. Zo kunnen bijvoorbeeld alleen beheerders de configuratie van de webserver aanpassen, terwijl medewerkers enkel toegang krijgen tot functionaliteiten die passen bij hun rol. Gasten krijgen een beperkte, informatieve weergave te zien (Microsoft, 2025a).

## Network Security Group (NSG)

Om de netwerken binnen Azure af te schermen van onbevoegde toegang, worden er voor Vlammend Varken beveiligingsregels per subnet ingesteld. De Network Security Group wordt gebruikt om netwerkverkeer van en naar Azure-resources in een virtueel netwerk te filteren. Hiermee wordt ongewenst verkeer effectief geblokkeerd. (Microsoft, 2025d)

## Azure Firewall

Om externe bedreigingen te detecteren en blokkeren, wordt gebruikgemaakt van de Azure Firewall. Deze bewaakt al het inkomend verkeer van buiten naar het interne netwerk, wat ook wel noord-zuidverkeer wordt genoemd, en fungeert als eerste verdedigingslinie tegen aanvallen (Microsoft, 2025c).

Om bedreigingen van buitenaf te detecteren en hiertegen te beschermen wordt de firewall ingezet. Alle netwerkverkeer van buitenaf naar het interne netwerk wordt ook wel Noor-Zuid verkeer genoemd. (Microsoft, 2025c)

## Back-up & Recovery

Om dataverlies bij incidenten te voorkomen, is een back-up- en herstelmachine ingericht. Mocht er een technisch probleem optreden, dan kunnen gegevens worden hersteld vanaf een recente back-up. Hiermee wordt continuïteit van de dienstverlening gewaarborgd.

## Logging

Voor het kunnen aantonen van verantwoord gebruik en het controleren van beveiligingsmaatregelen is logging onmisbaar. Het systeem houdt bij wie verbinding maakt met de webserver of een poging daartoe doet. Deze gegevens kunnen worden gebruikt voor foutopsporing, beveiligingsonderzoeken en naleving van interne regels.

## Private Endpoint Connection(s)

Via Private Endpoint Connection(s) kunnen interne onderdelen van het netwerk, zoals de beheer-VM, veilig communiceren met bijvoorbeeld de SQL-database of de API-VM. Deze verbindingen verlopen volledig via private netwerken en worden niet blootgesteld aan het openbare internet (Microsoft, 2025e).

## VPN Gateway

Voor beheerders is een Virtual Private Network (VPN) Gateway ingericht, waarmee zij vanaf hun eigen locatie op een veilige manier verbinding kunnen maken met het interne netwerk van Vlammend Varken. Zo kunnen ze systeemonderhoud uitvoeren zonder fysiek op locatie te zijn.

# Proof of Concept (POC)

Voor het Proof of Concept is het volledige proces van de gast als uitgangspunt genomen. Daarbij is onderzocht hoe het menu toegankelijk wordt gemaakt via de webserver, hoe de communicatie met de database plaatsvindt, en welke beveiligingsmaatregelen nodig zijn om dit proces veilig en stabiel te laten verlopen. Het doel was om de technische haalbaarheid van deze keten aan te tonen binnen een cloudgebaseerde infrastructuur op Microsoft Azure.

## Gerealiseerde onderdelen

In het POC zijn de volgende componenten succesvol opgezet en getest:

* Een virtueel netwerk bestaande uit meerdere subnets met per subnet een eigen Network Security Group.
* Toegang tot een beheerder-VM via een VPN Gateway.
* Een webserver (PaaS) die communiceert met een API-VM.
* Een API Management-service die het verkeer tussen de webserver en de API-VM beheert, inclusief loggingfunctionaliteit.
* Een API-VM die gegevens ophaalt uit de SQL-database binnen een beveiligd subnet.
* Een SQL-server en database die zijn ondergebracht in een afgeschermd subnet.
* Private Endpoints die veilige communicatie tussen de subnets mogelijk maken.

## Beperkingen

Een aantal functionaliteiten brengt extra kosten met zich mee, wat beperkingen opleverde binnen het huidige account. Hierdoor konden onderdelen zoals Entra ID niet volledig worden ingezet. Ook zijn beveiligingscomponenten zoals Azure Firewall, APIM en Microsoft Defender pas laat geconfigureerd om kosten te beperken.

# Bibliografie

Microsoft. (2025a, maart 4). *What is Microsoft Entra authentication?* Opgehaald van Microsoft Learn: https://learn.microsoft.com/en-us/entra/identity/authentication/overview-authentication

Microsoft. (2025b, januari 31). *What is enterprise user management?* Opgehaald van Learn Microsoft: https://learn.microsoft.com/en-us/entra/identity/users/directory-overview-user-model

Microsoft. (2025c, maart 19). *What is Azure Firewall?* Opgehaald van Learn Microsoft: https://learn.microsoft.com/en-us/azure/firewall/overview

Microsoft. (2025d, april 30). *Hoe netwerkbeveiligingsgroepen netwerktrafiek filteren.* Opgehaald van Learn Microsoft: https://learn.microsoft.com/nl-nl/azure/virtual-network/network-security-group-how-it-works

Microsoft. (2025e, april 2). *Wat is Azure Private Link?* Opgehaald van Microsoft Learn: https://learn.microsoft.com/nl-nl/azure/private-link/private-link-overview