A group of people sitting at a table

Description automatically generated with medium confidence

**Lab Journal**

**Booking.com**



Namen: Abraham Joseph, Bas Boelens

Klas: ITVN2

Groep: N2G5

E-mail: [a.joseph@st.hanze.nl](mailto:a.joseph@st.hanze.nl) [b.boelens@st.hanze.nl](mailto:b.boelens@st.hanze.nl)

# Inhoudsopgve

[Oriëntatie 3](#_Toc160474784)

[Bedrijfsflags verzamelen 3](#_Toc160474785)

[Flag 1 – shodan search 3](#_Toc160474786)

[Flag 2 – test sub-domain 4](#_Toc160474787)

[Flag 3 – ticketsysteem & outdated pagina 4](#_Toc160474788)

[Flag 4 – learning subdomain voor medewerkers 5](#_Toc160474789)

[5](#_Toc160474790)

[Flag 5 – dns records 5](#_Toc160474791)

[Flag 6 – Kassasysteem Eijsink 6](#_Toc160474792)

[Flag 7 – Single sourcing 6](#_Toc160474793)

[Flag 8 – tools en software die gebruikt wordt door booking.com 7](#_Toc160474794)

[Interessante informatie 7](#_Toc160474795)

[Profiel van een medewerker 8](#_Toc160474796)

[Pretext 9](#_Toc160474797)

[Phishing mail 10](#_Toc160474798)

# Oriëntatie

Booking.com, gevestigd aan de Oosterdokskade 163 in Amsterdam, is een toonaangevend bedrijf in de online reisbranche. Met een indrukwekkend personeelsbestand van 21.600 medewerkers, varieert de werkomgeving van fysieke locaties tot een hybride model waarbij medewerkers zowel op kantoor als op afstand werken. Om de samenwerking te bevorderen, stimuleert Booking.com zijn medewerkers om minimaal twee keer per week op kantoor aanwezig te zijn, waar elk team of afdeling toegewezen ruimtes heeft.

Het bedrijf beheert niet alleen de eigen kantoren, maar ook drie restaurants op de Booking.com Campus. Deze faciliteiten worden beheerd door zowel interne medewerkers als externe leveranciers voor schoonmaak, catering en beveiliging. Bovendien heeft Booking.com een speciale werkomgeving gecreëerd voor medewerkers die op afstand werken, waardoor er een flexibele en inclusieve werkcultuur ontstaat, deze omgeving wordt beheerd door een softwarebedrijf genaamd Miro.

Wat betreft ICT-services en infrastructuur heeft Booking.com een datacenter in Amsterdam, essentieel voor het waarborgen van de betrouwbaarheid en snelheid van hun diensten. Het onderhoud en beheer van de servers wordt verzorgd door Unica, een bedrijf in Amsterdam.

# Bedrijfsflags verzamelen

## Flag 1 – shodan search

Afbeelding met tekst, software, schermopname

Automatisch gegenereerde beschrijving

Afbeelding met tekst, schermopname, Lettertype

Automatisch gegenereerde beschrijving

**Wat is de informatie:** In de bovenstaande screenshots worden zowel de SSL-Certificates als de gebruikte servers weergegeven.

**Waar:** Deze informatie is verkregen door het gebruik van Shodan, hier werd vervolgens gezocht op “Booking” en “ Booking.com”.

**Risicoanalyse:** Potentiële impact is laag. Een aanvaller zou met deze gegevens een vals certificaat kunnen genereren. Ook kan het invloed hebben op de publiekelijke bekendheid.

**Oplossing:** overwegen nieuwe certificaat genereren en beveiliging zo optimaliseren dat deze gegevens niet makkelijk zichtbaar zijn voor mensen met slechte intenties.

## Flag 2 – test sub-domain

A screenshot of a computer

Description automatically generated

**Wat is de informatie:** booking.com heeft een test domain die waarschijnlijk voor test doeleinde wordt gebruikt. De server vraagt zelf om het wachtwoord in plaats van een inlog pagina of externe partij. Heeft geen limiet voor hoe vaak je het wachtwoord kan raden.

**Waar:** sub-domains bekijken van booking.com en focus leggen op de test en playground. Pagina maakt ook gebruik van derde-partijen domains. <https://test.partner.booking.com>

**Risicoanalyse:** impact is hoog. Aanvaller kan toegang krijgen tot een accountdoormiddel van een bruteforce.

## A screenshot of a login form Description automatically generatedA screenshot of a website Description automatically generatedFlag 3 – ticketsysteem & outdated pagina

A screenshot of a computer

Description automatically generated

Afbeelding met tekst, Lettertype, schermopname, informatie

Automatisch gegenereerde beschrijving

**Wat is de informatie:** informatie over welke software er gebruikt wordt voor booking.com helpdesk (Zendesk) & oude niet werkende zendesk pagina

**Waar:** informatie gevonden op <https://startup.jobs/zendesk-administrator-bookingcom-326329> extra informatie over oude zendesk page van booking.com oude pagina is gevonden doormiddel van een oude ticket https://booking-zen-5.zendesk.com/

**Risicoanalyse:** impact is laag. Een potentiële aanvaller zou verschillende tools kunnen gebruiken om de oude site te hacken, sinds deze niet goed functioneert en up-to-date is.

## Flag 4 – learning subdomain voor medewerkers

A screenshot of a login form

Description automatically generated

## A screenshot of a computer Description automatically generatedA computer with stickers on it Description automatically generated

**Wat is de informatie:** subdomain voor medewerkers die focust op het leren binnen het bedrijf. Oude domain was: learning.booking.com deze link forward automatisch naar een nieuwe derde-partij <https://bookingholdings.okta.com>.

**Waar:** heb deze informatie kunnen vinden doormiddel van een stikker van een medewerker. Deze stikker stond op een laptop van een medewerker die op youtube werd geïnterviewd.

**Risicoanalyse:** Potentiele impact is laag. Beveiliging van de derde-partij is wat lager dan die van booking.com. Certificaat type en algoritme is ook duidelijk vindbaar. Een aanvaller zou doormiddel van deze gegevens poging kunnen doen op cracken en de encryptie.

## Flag 5 – dns records

Afbeelding met tekst, Lettertype, schermopname, informatie

Automatisch gegenereerde beschrijving

Afbeelding met tekst, schermopname, Lettertype, Elektrisch blauw

Automatisch gegenereerde beschrijving

Afbeelding met tekst, Lettertype, schermopname, lijn

Automatisch gegenereerde beschrijving

Afbeelding met tekst, schermopname, Lettertype, lijn

Automatisch gegenereerde beschrijving

**Wat is de informatie:** Dit zijn DNS records van booking.com

**Waar:** DNShistory

**Risicoanalyse:** Redelijk gevaarlijk aangezien een aanvaller kan zien welke software/tooling er gebruikt wordt en dus deze zwakke punten makkelijk kan exploiteren.

**Oplossing:** DNS records hidden maken.

## Flag 6 – Kassasysteem Eijsink

Afbeelding met kop, tafelgerei, tafel, Drinkgerei

Automatisch gegenereerde beschrijvingAfbeelding met tekst, schermopname, Lettertype

Automatisch gegenereerde beschrijving

**Wat is de informatie:** Het kassasysteem van Bookinh.com die in het hele gebouw wordt gebruikt.

**Waar:** youtube.com video van een vlogger in booking.com hoofdkantoor Amsterdam.

**Riscoanalyse:** Impact kan groot zijn. Als Eijsink een storing of een bekende bug heeft dan kunnen hackers hier gebruik van maken.

**Oplossing:** medewerkers en gasten mogen niet zomaar vlogen in het gebouwd, onnodige labels en stikker van belangrijke apparatuur verwijderen.

## Flag 7 – Single sourcing

Afbeelding met tekst, schermopname, Lettertype

Automatisch gegenereerde beschrijving

**Wat is de informatie:** Marnix zegt hier dat booking.com derde partijen gebruikt voor onderanderen beveiliging, schoonmaak en catering. Booking.com wil voornamelijk alles zelf regelen.

**Waar:** [Nieuw hoofdkantoor Booking.com (65.000 m2): magneet voor eigen medewerkers én jong talent (facto.nl)](https://www.facto.nl/33590/nieuw-hoofdkantoor-booking-com-65-000-m2-magneet-voor-eigen-medewerkers-en-jong-talent)

**Risicoanalyse:** risico is laag. Booking.com wilt voornamelijk alles zelf regelen, dit kan betekenen dat zij voor de ICT-gerelateerde zaken hun medewerkers liever gebruiken dan een derde partij die gespecialiseerd is in security.

**Oplossing:** gespecialiseerde bedrijven inhuren voor het security gedeelte van

## Flag 8 – tools en software die gebruikt wordt door booking.com

Afbeelding met tekst, schermopname, Lettertype, brief

Automatisch gegenereerde beschrijving

**Wat in de informatie:** alle tools en software die booking.com gebruikt

**Waar:** <https://rocketreach.co/company?name=Booking.com>

**Risicoanalyse:** risico is laag. Aanvaller hebben hier door inzicht in de applicaties die gebruikt worden door booking.com waardoor zijn hun aanvallen kunnen focussen op een software of tool die bekendstaat om bugs en problemen.

**Oplossing:** Zoveel mogelijke tools en software gesloten houden.

## Afbeelding met gebouw, kleding, persoon, Reinheid Automatisch gegenereerde beschrijvingInteressante informatie

A computer with a screen on

Description automatically generated

Afbeelding met tekst, schermopname, Lettertype, lijn

Automatisch gegenereerde beschrijvingAfbeelding met tekst, schermopname, software, Website

Automatisch gegenereerde beschrijving

Afbeelding met tekst, Lettertype, schermopname, lijn

Automatisch gegenereerde beschrijvingAfbeelding met tekst, schermopname, Lettertype

Automatisch gegenereerde beschrijvingAfbeelding met tekst, schermopname, Lettertype

Automatisch gegenereerde beschrijvingAfbeelding met tekst, schermopname, Lettertype

Automatisch gegenereerde beschrijving

## Samenvatting flags

Booking.com, een vooraanstaand online reisplatform, hebben wij onderzocht op hun internetbeveiliging. Het verkregen inzicht onthult verschillende aspecten van hun online aanwezigheid en beveiligingsstructuur.

Als een dynamisch en open bedrijf, bleek uit online video's dat Booking.com medewerkers hun dagelijks leven deelden. Deze video's boden ook zicht op de laptops die door de medewerkers werden gebruikt. Opvallend was dat werknemers onbedoeld veel informatie blootgaven, mogelijk zonder medeweten van de beveiligingsafdeling van Booking.com. Daarom hebben we ons gericht op de werknemers en ontdekt dat ze onbewust belangrijke informatie deelden, zoals sub-domeinen voor training, beheerd door derden, stickers van het kassasysteem, en interne security in het booking.com gebouw.

Hoewel Booking.com over sterke beveiligingsmaatregelen beschikt, hebben we door te focussen op werknemers toch kwetsbaarheden ontdekt. Onze verzamelde flags, met name afkomstig van werknemers, bieden een gedetailleerd beeld van Booking.com en onthullen specifieke zwakheden, met name op het gebied van werknemers en sociale media. Met dit profiel kunnen we phishing-e-mails richten op werknemers die actief zijn op sociale platforms.

Top of Form

Bottom of Form

# Profiel van een medewerker

[(15) Marnix Mali | LinkedIn](https://www.linkedin.com/in/marnixmali/?originalSubdomain=nl)

Onderstaande screenshots geven het LinkedIn profiel van Marnix Mali weer. Marnix is de director of real estate en workspace services bij booking.com.

Afbeelding met tekst, Lettertype, schermopname

Automatisch gegenereerde beschrijving

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

Afbeelding met tekst, schermopname, Lettertype

Automatisch gegenereerde beschrijving

Figure 1 Dit is de werkervaring van Marnix binnen Booking.com

**Heeft de medewerker recentelijk (of in de nabije toekomst) trainingen gehad?**

Afbeelding met tekst, Lettertype, schermopname, Graphics

Automatisch gegenereerde beschrijving

Figure 2 dit is een training die Marnix heeft gevolgd.

**Wat zijn het interne telefoonnummer & e-mailadres van de medewerker?**



Figure 3 Hier worden zijn zowel persoonlijke als werk-emails weergegeven.

[RocketReach Search - Find Email, Phone & Social Media](https://rocketreach.co/person?start=1&pageSize=10&link=https:%2F%2Fwww.linkedin.com%2Fin%2Fmarnixmali)

**Wat is de routine van de werknemer (start/eindtijden, pauzes, etc.)?**

Afbeelding met tekst, schermopname, Lettertype, nummer

Automatisch gegenereerde beschrijving

[Beeldbank (archief.amsterdam)](https://archief.amsterdam/beeldbank/detail/f7b7ffba-168d-a909-e6e4-c60897eca480)

**Werkt de medewerker veelal thuis of op kantoor?**

**Is de medewerker vaak op zakenreis? Waar naartoe?**

Op dit moment verblijft Marnix in Singapore. Dit houdt in dat hij zeer waarschijnlijk alles online doet qua werk.

Marnix is een interessant persoon om een aanval op uit te voeren. Hij heeft een redelijk hoge positie binnen Booking.com, maar is niet IT-gespecialiseerd. Dit houdt in dat hij waarschijnlijk wel toegang heeft tot interessante informatie, maar niet getraind is om oplettend te zijn tegenover een phishing-mail, in tegenstelling tot een IT-specialist. Deze IT-specialist zou meer interessante informatie bezitten, maar zou ook veel oplettender zijn voor dit soort aanvallen.

## Samenvattings profiel

Marnix Mali is een sleutelfiguur binnen Booking.com, met een indrukwekkende staat van dienst van 11 jaar en 3 maanden bij het bedrijf. Hij bekleedt momenteel de functie van Real Estate & Workspace Services Director, waarbij hij verantwoordelijk is voor de fysieke werkomgeving van het bedrijf.

Wat Marnix een aantrekkelijk doelwit maakt voor een phishing-aanval, is zijn positie en zijn gebrek aan specialisatie op het gebied van IT. Hoewel zijn hoge positie suggereert dat hij toegang heeft tot waardevolle informatie, duidt zijn niet-technische achtergrond erop dat hij wellicht minder bedachtzaam is tegenover phishing-e-mails in vergelijking met een IT-specialist.

Belangrijke aandachtspunten voor een phishing-aanval op Marnix zijn onder meer zijn niet-specialistische achtergrond in IT, zijn rol als Real Estate & Workspace Services Director, zijn recente verhuizing naar Singapore en zijn regelmatige onlineactiviteiten. Daarnaast zou de aanval moeten inspelen op zijn persoonlijke interesses, zoals zijn kunstliefhebberij.

De gevonden flags, met name die gerelateerd aan de werknemers van Booking.com en zwakheden in de beveiliging, kunnen worden benut om een geloofwaardige en aantrekkelijke phishing-e-mail te creëren. Het doel is om Marnix te verleiden tot het klikken op een kwaadaardige link, waardoor vertrouwelijke informatie kan worden verkregen en verdere aanvallen op het bedrijf kunnen worden geïnitieerd.

# Pretext

Ik ben een Miro ICT-helpdesk medewerker. De persoon waarmee ik in contact sta is Marnix Mali. Hij is de Director of Real Estate & Workspace Services bij Booking.com. Hij verblijft op dit moment in Singapore.

## Sterke punten

### Geloofwaardigheid

De keuze voor een Miro ICT-helpdesk medewerker die een update voor de virtuele werkomgeving moet uitvoeren, geeft de aanval geloofwaardigheid. Het sluit aan bij Marnix Mali's functie en speelt in op mogelijke

### Noodzaak

Het inspelen op de noodzaak van een beveiligingsupdate creëert urgentie. Mensen zijn geneigd snel te handelen als het gaat om de veiligheid van hun gegevens en werkomgeving.

## Persoonlijke context

Door de naam, positie en locatie van Marnix Mali te gebruiken, wordt een persoonlijke context gecreëerd. Dit verhoogt de kans dat Marnix zich specifiek aangesproken voelt en minder alert is op verdachte signalen.

## Zwakke punten

Niet gespecialiseerd in IT

Marnix Mali wordt omschreven als niet gespecialiseerd op het gebied van IT. Hoewel dit een geen zwak punt is voor Marnix, is het wel een risico voor ons, omdat hij mogelijk geen verstand hiervan heeft een wellicht deze verzoek doorstuurt naar zijn IT-afdeling in Singapore.

Vertrouwen in de afzender

Hoewel het gebruik van "noreply@miro.com" de indruk wekt dat het een legitieme geautomatiseerde e-mail is, kan het ook argwaan wekken als Marnix gewend is aan andere communicatiekanalen of als de e-mail niet overeenkomt met het gebruikelijke patroon.

## Conclusie

Gezien de genoemde sterke punten en zwakke punten, lijkt de successkans redelijk hoog. Het creëren van een geloofwaardige context en het benutten van urgentie vergroten de kans dat Marnix op de link klikt. Toch kunnen het gebrek aan IT-kennis en eventuele argwaan bij vreemde e-mailadressen de aanval bemoeilijken.

# Phishing mail

Onderwerp: Belangrijk: Veiligheidsupdate Miro Applicatie vanwege Verhuizing Booking.com Hoofdkantoor

Beste Marnix,

Wij hopen dat deze e-mail u in goede gezondheid bereikt. Graag willen wij u op de hoogte stellen van een dringende veiligheidsupdate voor de Miro-applicatie op uw apparaat, die verband houdt met de aanstaande verhuizing van het Booking.com hoofdkantoor in Amsterdam.

In het kader van onze voortdurende inzet om de prestaties en beveiliging van onze software te verbeteren, hebben we onlangs een nieuwe versie van de Miro-app uitgebracht. Deze update bevat niet alleen bugfixes en prestatieverbeteringen, maar ook cruciale veiligheidsupdates om ervoor te zorgen dat uw gegevens en de app beschermd blijven, met name tijdens de overgangsperiode van de verhuizing.

U kunt de update direct downloaden vanaf onze officiële updatepagina: [<https://miro.com/nl/apps/> (Link met virus)]

Wij begrijpen dat uw tijd kostbaar is, maar we benadrukken het belang van deze update voor de integriteit van uw gegevens en de goede werking van de app, vooral gezien de veranderingen die de verhuizing met zich meebrengt.

Als u vragen heeft of hulp nodig heeft bij het bijwerken van de app, staan wij voor u klaar. Aarzel niet om contact met ons op te nemen via [support@miro.com([fake\_link])](mailto:support@miro.com([fake_link]))

Bedankt voor uw begrip en medewerking.

Met vriendelijke groet,

Het Miro Support Team

noreply@miro.com