



Lab Journal Booking.com

Namen: Abraham Joseph, Bas Boelens
Klas: ITVN2
Groep: N2G5
E-mail: a.joseph@st.hanze.nl b.boelens@st.hanze.nl

share your talent. **move** the world.

Inhoudsopgave

<i>Oriëntatie</i>	3
<i>Bedrijfsflags verzamelen</i>	3
Flag 1 – shodan search.....	3
Flag 2 – test sub-domain.....	4
Flag 3 – ticketsysteem & outdated pagina	4
Flag 4 – learning subdomain voor medewerkers.....	5
.....	5
Flag 5 – dns records	5
Flag 6 – Kassasysteem Eijsink.....	6
Flag 7 – Single sourcing.....	6
Flag 8 – tools en software die gebruikt wordt door booking.com	7
Interessante informatie	7
<i>Profiel van een medewerker</i>	8
<i>Pretext</i>	11
<i>Phishing mail</i>	12

Oriëntatie

Booking.com, gevestigd aan de Oosterdokskaade 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

The screenshot displays a Shodan search result for the domain booking.com. The top section shows the SSL certificate details, including the issuer (DigiCert Global G2 TLS RSA), the organization (Booking.com BV), and the supported SSL versions (TLSv1.2, TLSv1.3). The bottom section shows an HTTP 421 Misdirected Request error from the Envoy server, with a message indicating that the service is not registered for this consumer.

```
HTTP/1.1 421 Misdirected Request
x-bookings-controlplane-error-reason: service not registered for this consumer
content-length: 40
content-type: text/plain
date: Thu, 15 Feb 2024 12:32:01 GMT
server: envoy
x-xss-protection: 1; mode=block
strict-transport-security: max-age=604800; includeSub...
```

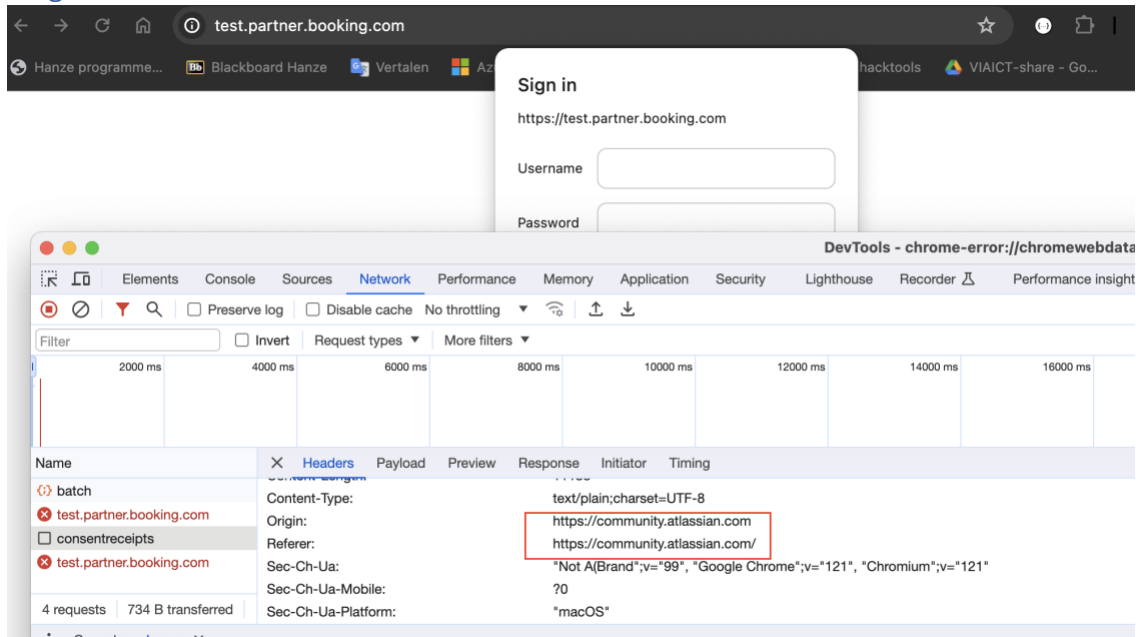
Wat is de informatie: In de bovenstaande screenshots worden zowel de SSL-Certificates als de gebruikte servers weergegeven.

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

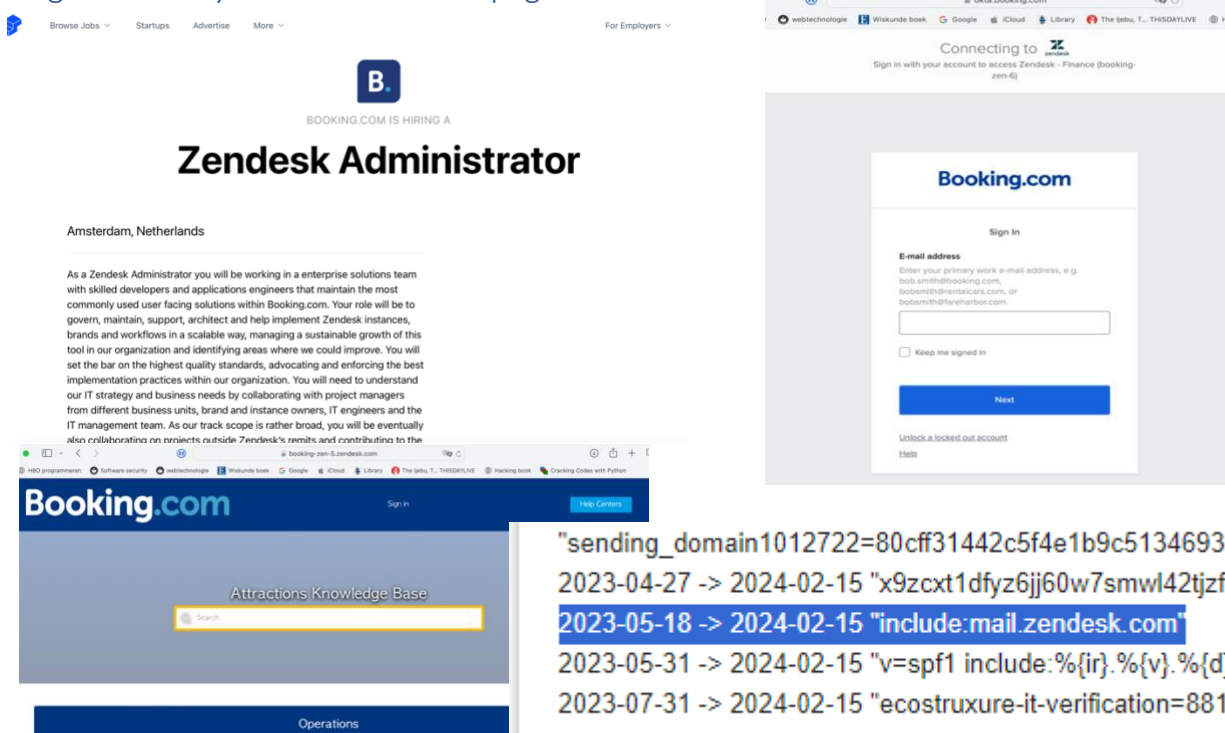


Wat is de informatie: booking.com heeft een test domain die waarschijnlijk voor test doeleinde wordt gebruikt. De server vraagt zelf om het wachtwoord in plaats van een inlog pagina of externe partij. Heeft geen limiet voor hoe vaak je het wachtwoord kan raden.

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.

Flag 3 – ticketsysteem & outdated pagina



"sending_domain1012722=80cff31442c5f4e1b9c51346939d5bf2
2023-04-27 -> 2024-02-15 "x9zcxt1dfyz6jj60w7smwl42tjzfv5yn"
2023-05-18 -> 2024-02-15 "include:mail.zendesk.com"
2023-05-31 -> 2024-02-15 "v=spf1 include:%{ir}:%{v}:%{d}.spf.h
2023-07-31 -> 2024-02-15 "ecostruxure-it-verification=881dfd3b-

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

Connecting to **docebo**
Sign in with your account to access Docebo

BOOKING HOLDINGS

Sign In


Primary Email

This field cannot be left blank.

☐ Keep me signed in

Next

Help



<https://bookingholdings.okta.com/> Monitor This

Certificate

Primary

Common Name: *.okta.com

- Issuer: DigiCert TLS RSA SHA256 2020 CA1
- Expires: 57 days
- Valid From: 5/21/2023
- Valid To: 4/12/2024
- Serial: 0A99C132DFD806FEF9E3C5A35793B4B
- Algorithm: sha256RSA
- Organization: Okta, Inc.
- Location: San Francisco, California, US

Common Name: DigiCert TLS RSA SHA256 2020 CA1

- Issuer: DigiCert Global Root CA
- Expires: 7 years
- Valid From: 9/23/2020
- Valid To: 9/23/2030
- Serial: 0A3508D55C292B017DF8AD65C00FF7E4
- Algorithm: sha256RSA
- Organization: DigiCert Inc
- Location: US

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 sticker van een medewerker. Deze sticker 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

```
"sending_domain1012722=80cff31442c5f4e1b9c51346939d5bf2
2023-04-27 -> 2024-02-15 "x9zcx1dfyz6jj60w7smwl42tjzfv5yn"
2023-05-18 -> 2024-02-15 "include:mail.zendesk.com"
2023-05-31 -> 2024-02-15 "v=spf1 include:%{ir}:%{v}:%{d}.spf.ha
2023-07-31 -> 2024-02-15 "ecostruxure-it-verification=881dfd3b-
el27sV3TBfQVLBPHGWHiins"
2022-08-25 -> 2024-02-15 "Dynatrace-site-verification=3a88fc1a-195c-455d-ab87-
88d09191496b__drhtlct978bncn9utek6qdqapk"
2022-08-25 -> 2024-02-15 "google-site-
2022-08-25 -> 2024-02-15 "docusign=1ddc2bf3-a249-4127-a351-f22dc75077d3"
2022-08-25 -> 2024-02-15 "miro-verification=a08b425a7aa0b2b93256f4b504ee72afe8f9e0b9"
2022-08-25 -> 2024-02-15 "ZOOM_verify_rRPrFA9oTH2bxfFkJJeQTzA"
2022-08-25 -> 2024-02-15 "atlassian-domain-
verification=PEQekniknTLbMzMw6lfb9G9YWzhgcGHZlne34xYo7zW9/rzVsM/6qZSUWdIVAmR"
2023-05-31 -> 2024-02-15 v=spf1 include:%{ir}:%{v}:%{d}.spf.ha.ppnrosted.com -all
2023-07-31 -> 2024-02-15 "ecostruxure-it-verification=881dfd3b-5776-4fc0-a5f6-190a0ac842f8"
2023-10-31 -> 2024-02-15 "modell-verify-1764xQVEQ12x076WCHz"
```

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



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.

Risicoanalyse: 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 vloggen in het gebouw, onnodige labels en sticker van belangrijke apparatuur verwijderen.

Flag 7 – Single sourcing

Bewuste keuze voor single sourcing

De facilitaire services in de Booking.com Campus worden geleverd door zowel eigen medewerkers, zoals hospitality-medewerkers en office medewerkers, als medewerkers van leveranciers van onder meer de schoonmaak, catering en security.

Belangrijk aandachtspunt in de relatie met de leverancier is het betrekken van de inhuurmedewerkers bij de organisatie, vertelt Mali. 'Het vraagt extra inzet van onze kant, maar het is beslist zinvol omdat die medewerkers zich dan meer betrokken voelen, beter presteren enzovoort.'

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 \(facto.nl\)](#)

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

Technologies
JavaScript, HTML, PHP, Twitter, Google Analytics, Font Awesome, Google Tag Manager, Nginx, G Suite, Polyfill, Bootstrap, jQuery, ASP.NET, YouTube, Google Maps, Microsoft Outlook, Gmail, Yoast Plugins, Facebook, Apache, Apache HTTP Server, Github, Facebook Pixel, jQuery UI, Facebook Pixel For Shop, Google Doubleclick, Amazon S3, Amazon CloudFront, Amazon Web Services (AWS), Wordpress, Slack, Instagram, NodeJS, Adobe, PayPal, New Relic, LinkedIn Login, Google Drive, Microsoft Office, Twitter Analytics, HubSpot, Hotjar, Google Calendar, Google Translate, Microsoft Azure, Adyen, Microsoft Office 365, Stripe, Backbone.js, Microsoft SQL Server, Linux, Zoom, Drupal, Microsoft Excel, Python, MySQL, Zendesk, Java, Laravel, Microsoft Project, Pivotal, React, Google Cloud Platform, Desk.com Chat, SendGrid, Adobe Illustrator, Google Sites, Adobe Marketing Cloud, AngularJS, Salesforce CRM, Teamwork, Microsoft Word, WP Engine, VMware, Facebook Apps and Tabs, QuickBooks, SSL.com, Drupal 7, Testpilot, Microsoft SharePoint, Git, Microsoft Access, JIRA Software, RequireJS, Wix, Adobe Photoshop, Microsoft Teams, Vue.js, Atlassian JIRA, Facebook for Business, Google Ads, Google Sheets, Microsoft Azure DNS, Review Board, Adp, The Receptionist, Microsoft Dynamics, Tableau Software, Microsoft Active Directory, My Hours (Show fewer)

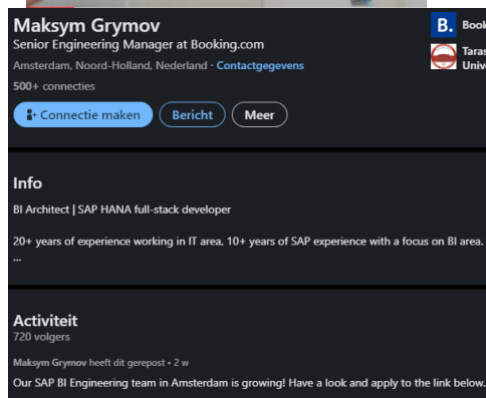
Wat in de informatie: alle tools en software die booking.com gebruikt

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.

Interessante informatie



Werkplekconcept en vloerindeling

Sinds de overgang naar hybride werken worden medewerkers van Booking.com aangemoedigd om minstens twee dagen per week op kantoor te werken. Ze kunnen overal in het gebouw gebruik maken van de vele flexplekken. Iedere afdeling of team heeft wel een vaste 'plek' toegewezen gekregen.

Bewuste keuze voor single sourcing

De facilitaire services in de Booking.com Campus worden geleverd door zowel eigen medewerkers, zoals hospitality-medewerkers en office medewerkers, als medewerkers van leveranciers van onder meer de schoonmaak, catering en security.

Bela Managing agent of IFM?

Of Mali nog heeft nagedacht om met een ander besturingsmodel te gaan werken, zoals managing agent of IFM?
'We hebben alles overwogen, maar er bewust voor gekozen om zoveel mogelijk in eigen hand te houden. Wat je zelf niet beter kunt doen moet je outsourcen, dat is duidelijk. Maar we willen de aansturing echt zelf doen, zeker nu het hier allemaal nieuw is en voor willen zorgen dat de dienstverlening echt een ng.com-stempel krijgt.'

In het nieuwe kantoor van Booking.com bevinden zich drie restaurants. In een van de restaurants, namelijk het Chef's Restaurant, vindt er om de drie maanden een verandering plaats.

Bij wisseling van de seizoenen wordt een chef van naam en faam uitgenodigd om een bijzonder menu te bedenken dat in het restaurant geserveerd wordt.

Vlak voor de zomer, toen het kantoor net in gebruik werd genomen, was het eterraankolke Jorie Biddandijk bekend van onder

Aan het woord is **Marnix Mali**, Director Real Estate & Workspace Services (REWS) bij Booking.com.

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.

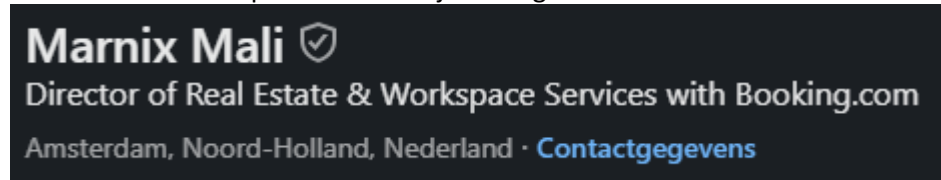
Als een dynamisch en open bedrijf, bleek uit online video's dat Booking.com medewerkers hun dagelijks leven deelden. Deze video's boden ook zicht op de laptops die door de medewerkers werden gebruikt. Opvallend was dat werknemers onbedoeld veel informatie blootgaven, mogelijk zonder medeweten van de 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.

Profiel van een medewerker

(15) [Marnix Mali | LinkedIn](#)

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



Hoe lang werkt de werknemer al bij het bedrijf?

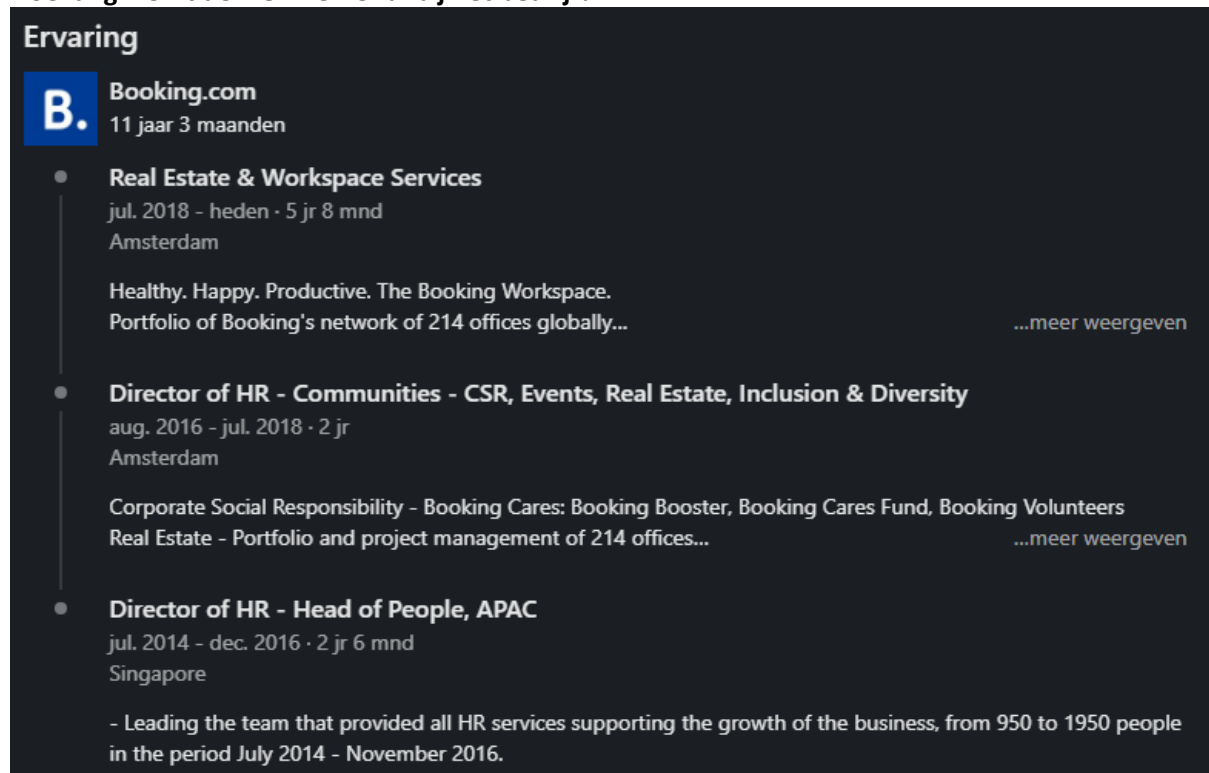


Figure 1 Dit is de werkervaring van Marnix binnen Booking.com

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

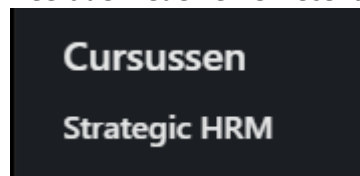


Figure 2 dit is een training die Marnix heeft gevolgd.

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](#)

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

Gegevens

Titel

Marnix Mali (49), HR-manager, Keizersgracht
(Grachtengordel)

Beschrijving

Zaterdagochtend, 11:00 uur. Foto uit de serie "Zaterdagochtend", gepubliceerd in Het Parool. Marnix Mali geniet nog een laatste keer van het ontbijt in zijn huis aan de Keizersgracht voor hij verhuist naar Singapore. Hij is HR-manager bij Booking.com. "Het was altijd al een wens van ons om in Azië te gaan wonen en werken. We komen regelmatig in Japan, waar mijn vrouw Yoshie Tokuno (44) vandaan komt", zegt Marnix. Baby Jiro zit voor het eerst 's ochtends aan tafel. Taro (6) ontbijt liever tussen zijn treinen. Hij is tweetalig opgevoed: Japans en Nederlands. "Gelukkig hebben we een Nederlandse school voor hem gevonden".

[Beeldbank \(archief.amsterdam\)](#)

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])

Bedankt voor uw begrip en medewerking.

Met vriendelijke groet,

Het Miro Support Team
noreply@miro.com