



18.04.2024

Vorbereitet auf NIS 2 ?!

DI Susanne EBM | Leitung Informationssysteme Flughafen Wien AG

Einblick in das Unternehmen Flughafen Wien



Einblick in das Unternehmen Flughafen Wien

Entwickler, Errichter und Komplettbetreiber des Flughafen Wien:

- Operativer Flughafenbetrieb
- Bodenabfertigungsdienste
- Sicherheitsdienstleistungen
- Infrastrukturanbieter
- Kommerzielle Aktivitäten





Der Flughafen Wien in Zahlen

29,5 Mio.

Passagiere in 2023

111.500

Passagiere am stärksten
Tag (16.07.2023)



€ 931,5 Mio.

Umsatz in 2023

€ 188,6 Mio.

Periodenergebnis in 2023



606

Flüge / Tag



TOP 5

Destinationen Westeuropa

London – Frankfurt – Paris –
Istanbul – Amsterdam



12 km²

Gesamtfläche

245.000 t

Fracht in 2023



>5.000

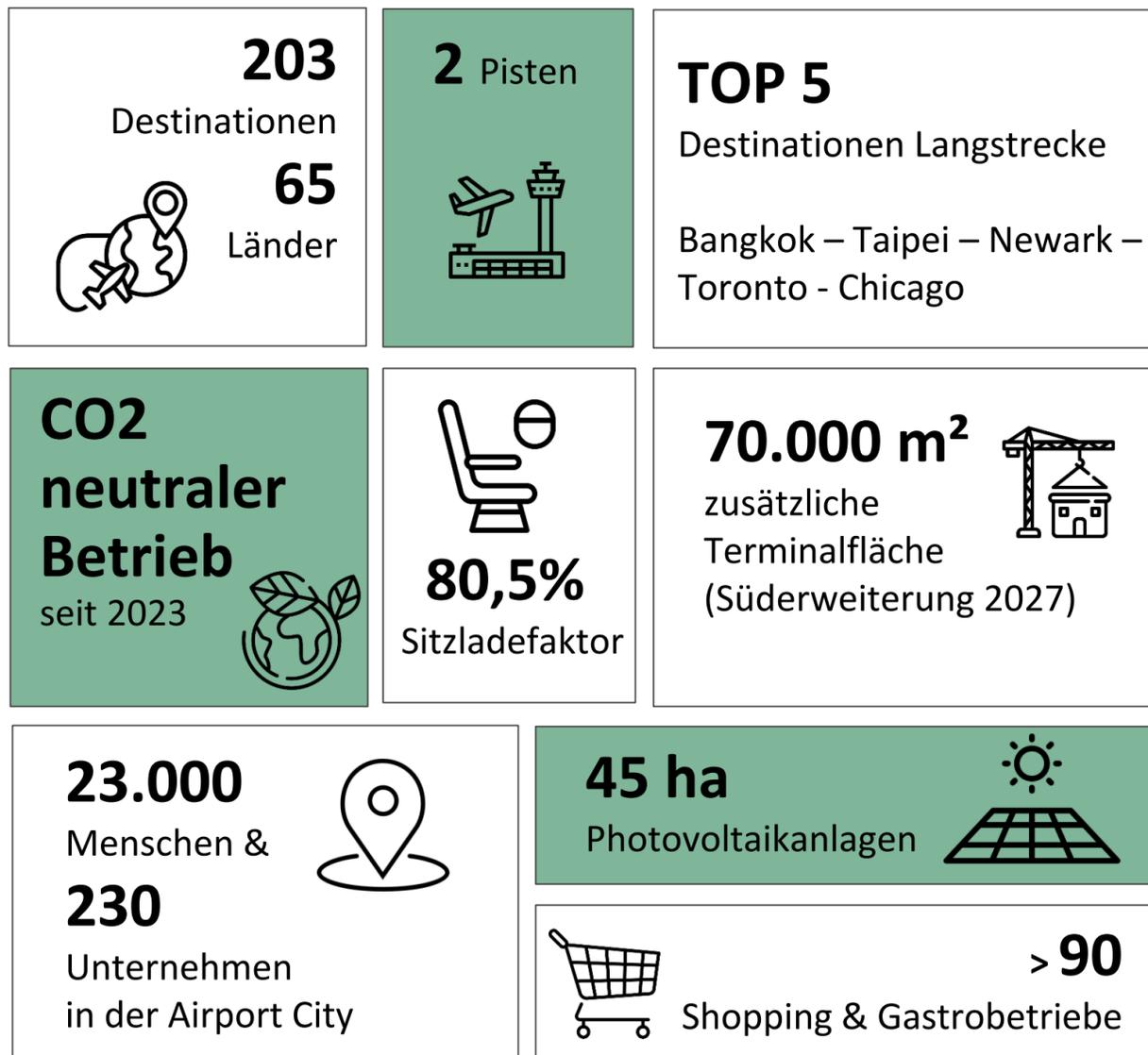
Mitarbeiter:innen



Pünktliches Drehkreuz

3. Platz in ganz Europa

Der Flughafen Wien in Zahlen



Wir betreiben IT für eine ganze Stadt





NIS



NIS 1 – Der Flughafen Wien als kritische Infrastruktur

- Der Flughafen Wien zählt wie rund 100 andere Unternehmen als „**Betreiber wesentlicher Dienste**“ zur **kritischen Infrastruktur** und fällt daher unter NIS 1
- Demnach sind IT-Gewerke, die **kritisch für Passagier- und Gepäckabfertigung sowie Sicherheitssysteme** sind, besonders zu schützen
- Dies wurde zum Anlass genommen, die vorhandene **Cyber Security** weiter auszubauen und ein **ISMS¹** zu etablieren
- Unser ISMS setzt **Mindeststandards in Bezug auf Cyber Security** und behandelt eine Vielzahl von Themengebieten wie technische Schutzmaßnahmen, Kryptografie, Lieferantenmanagement aber auch Mitarbeiterschulungen und Umgang mit Notfällen/Krisen

¹ Information Security Management System

Was bedeutet NIS 2 konkret für den Flughafen?

Unterschiede im Anwendungsbereich:

NIS 1

- Jene IT-Systeme, die zur Durchführung der Passagier- und Gepäckabfertigung sowie zum Betrieb der Sicherheitssysteme erforderlich sind
- Aufnahme dieser kritischen Systeme ins ISMS der Flughafen Wien AG

NIS 2

- Alle IT-Systeme der Flughafen Wien AG müssen betrachtet und in Kontext mit den Unternehmenszielen gesetzt werden
- Hierzu wird eine Business Impact Analyse durchgeführt
- Basierend auf deren Ergebnisse werden die einzelnen IT-Gewerke behandelt

NIS 2 - Richtlinie

CHANCEN

- (Cyber-)Sicherheitsaspekt wird EU-weit gefördert
- Mindeststandards in Zusammenarbeit mit anderen Unternehmen sinnvoll
- Durch transparente und rechtzeitig publizierte Vorgaben können Unternehmen nachhaltig Mehrwert generieren

HERAUSFORDERUNGEN

- Balance Cybersicherheit & Wirtschaftlichkeit
- Gefahr überschießende Bürokratisierung
- „Prinzip Gießkanne“ führt zu Nivellierung nach unten
- Fokus auf „wesentliche Dienste“ wird durch NIS 2 aufgeweicht – vorhandene Ressourcen müssen auch auf „irrelevante“ Systeme verwendet werden

Das ISMS (Information Security Management System)

Gesamtheitliches System, um die **Integrität, Vertraulichkeit und Verfügbarkeit** unserer IT-Systeme und der darin verarbeiteten Daten sicherzustellen.

Einige Eckpfeiler:

- Zyklische Risikoidentifizierung (Risikointerviews & Pentests)
- Strukturierte und lückenlose Behandlung aller bekannten Risiken
- Reporting an die Geschäftsführung
- Cyber Security Roadmap
- Kontinuierlicher Verbesserungsprozess
- Mindeststandards etabliert
- Lieferantenmanagement
- Ereignismanagement
- Awareness Maßnahmen

Cyber Security Schulungen am Flughafen Wien

- **Regelmäßige, zielgruppenorientierte & verpflichtende Schulungen**
 - Basisschulung
 - Homeofficeschulung
 - Spezifische Schulungen (z.B. für Administratoren, Buchhaltung, HR)
 - Auffrischungsschulungen zu aktuellen Themen (z.B. Social Engineering)
- **Weitere Awareness Maßnahmen**
 - Simulierte Phishing-Mails
 - Intranet-Schaltungen
 - Benachrichtigungen bei besonderer Gefährdungslage

Ausblick für NIS 2 – was ist jetzt zu tun?

1. Die Gesetzestexte lesen und **tätig werden**
2. Unternehmensweit alle Prozesse betrachten und Kritikalität beurteilen (= **Business Impact Analyse**)
3. **ISMS** im Unternehmen ausrollen und etablieren
 - Risikoidentifizierung und –behandlung sicherstellen
 - Lieferantenmanagement implementieren
 - Awareness Maßnahmen durchführen
4. Dabei stets beachten – der **Fokus ist auf die kritischen Systeme** zu richten!
5. Rechtzeitig **registrieren (§29 NISG 2024)**





Unser Fazit nach 5 Jahren NIS

Lessons Learned

- Cyber Security ist ein **fortlaufender Prozess**
- Externe & interne **Audits** bringen Mehrwert!
- Strukturiertes **Risikomanagement** ist die halbe Miete
- Größten Risiken entstehen zwischen Bildschirm und Schreibtischsessel
- Hausverstand schlägt „Papiertiger“

Vielen Dank für Ihre Aufmerksamkeit!



DI Susanne EBM

Leitung Informationssysteme Flughafen Wien AG

✉ s.ebm@viennaairport.com