Flughafen Wien AG
Public Affairs
publicaffairs@viennaairport.com
Tel.: +43-1-7007-22222

Vienna International Airport

Datum: 15.10.2018
Zeichen: C/CP/TS/ts/227

Stellungnahme iRd Begutachtung des NISG

*Das Bundeskanzleramt hat am 19. September den Entwurf zum Netz- und Informationssystemsicherheitsgesetz (NISG), mit dem die NIS-Richtlinie (RL 2016/1148 (EU)) umgesetzt wird, übermittelt (**Geschäftszahl: BKA-180.310/0234-I/6/2018**). Die Flughafen Wien AG (FWAG) nimmt hiermit dazu Stellung.*

Einleitende Stellungnahme

Die Gewährleistung eines hohen Sicherheitsniveaus der Netz- und Informationssysteme ist im ureigenen Interesse des Flughafen Wien. Cybersecurity im weiteren Sinn hat in den vergangenen Jahren massiv an Bedeutung gewonnen, so wie auch insgesamt die Cyberattacken weltweit zugenommen haben. Der Flughafen Wien war selbst von solchen Attacken betroffen, konnte diese jedoch aufgrund der bereits bestehenden Schutzmechanismen abwehren (etwa im Sommer 2017).

Die NIS-RL bzw. das NISG ist somit ein wichtiger Schritt, der diesen Entwicklungen Rechnung trägt und zu einem allgemein hohen Sicherheitsniveau in Österreich und Europa beitragen kann. Wichtig ist dabei das sorgfältige Einbeziehen der betroffenen Unternehmen in den unterschiedlichen Sektoren. Denn einerseits betreiben die betroffenen Unternehmen (im Sinn des Gesetzes die „*Betreiber wesentlicher Dienste*“, kurz: BwD) in vielen Fällen bereits sehr ausgereifte Sicherheitssysteme. Zusätzliche Belastungen für Unternehmen sollten also möglichst gering gehalten werden. Andererseits sind die Gegebenheiten und Anforderungen je nach Sektor und Tätigkeit des BwD sehr spezifisch, weshalb maßgeschneiderte Lösungen notwendig sind. Das gilt für den Entwurf zum NISG ebenso wie für die noch auszustellenden Bescheide und Verordnungen.

Zum Entwurf des NISG

- **§9 Befugnisse zur Vorbeugung von Sicherheitsvorfällen**

In §9 wird die Möglichkeit für Betreiber wesentlicher Dienste (u.a.) angeführt, an vom BMI betriebenen technischen Einrichtungen teilzunehmen und festzulegen, welche Daten an den Bundesminister für Inneres übermittelt werden. Für die Teilnahme fallen entsprechende Kosten an, die dem BMI von den teilnehmenden BwD (u.a.) ersetzt werden sollen. Um Klarheit über den Charakter dieser Option zu schaffen, schlägt die FWAG vor, folgenden Satz am Ende von §9, Abs.1 zu ergänzen: ***„Die Teilnahme an den vom Bundesminister für Inneres betriebenen technischen Einrichtungen erfolgt für die Betreiber wesentlicher***

Dienste, Anbieter digitaler Dienste und Einrichtungen des Bundes auf freiwilliger Basis und kann für diese nicht verpflichtend vorgeschrieben werden."

- **§14 Ermittlung der Betreiber wesentlicher Dienste**

Bei der Ermittlung der BwD sollte sich der Bundekanzler jedenfalls an die in den Sektorengesprächen besprochenen Schwellenwerte halten, da diese in konstruktivem Diskurs zwischen den zuständigen Ministerien und den in den jeweiligen Sektoren betroffenen Unternehmen praxisnahe und realistisch behandelt wurden. Das sollte sich auch in den auszustellenden Bescheiden widerspiegeln.

- **§16 Meldepflichten für Betreiber wesentlicher Dienste**

§16 Abs. 4 ist missverständlich formuliert:
„(4) Nimmt ein Betreiber wesentlicher Dienste die Dienste eines Anbieters digitaler Dienste in Anspruch, so ist jede erhebliche Auswirkung auf die Verfügbarkeit der wesentlichen Dienste, die von einem den Anbieter digitaler Dienste beeinträchtigenden Sicherheitsvorfall verursacht wurde, von diesem Betreiber wesentlicher Dienste zu melden."

Aus Sicht der FWAG lässt diese Formulierung zumindest zwei Lesarten zu: Entweder würde das bedeuten, dass eine erhebliche Auswirkung auf die wesentlichen Dienste vorliegt, die ohnehin nach §16 zu melden ist. In diesem Fall ist dieser Absatz redundant und kann somit gänzlich gestrichen werden.
Oder dieser Absatz ist dahingehend zu deuten, dass ein BwD eine Meldung machen muss, die sich auf den Sicherheitsvorfall beim Anbieter digitaler Dienste bezieht. In diesem Fall handelt es sich für den BwD um eine „doppelte Meldepflicht", die sachlich nicht gerechtfertigt ist, da der Anbieter digitaler Dienste diese Meldung ohnehin nach §18 machen muss. Außerdem ist seitens des BwD gar nicht zu beeinflussen, ob für eine etwaige Meldung überhaupt Daten über den Sicherheitsvorfall in ausreichender Qualität vorliegen. Dann handelt es sich um eine Mehrbelastung für Betreiber wesentlicher Dienste, die aus Sicht der FWAG nicht gerechtfertigt ist.

In beiden Fällen spricht sich die FWAG für eine Streichung von §16 Abs. 4 aus. Sollten beide Interpretationen nicht der Intention des Gesetzgebers entsprechen, so sollte eine eindeutige Formulierung gesucht werden.

Die in **§16 Abs. 7 genannt Verordnung** sollte sich bei der Festlegung der Parameter des Sicherheitsvorfalls (siehe §3 Abs. 6 lit. a bis d) ebenfalls auf die in den Sektorengesprächen erzielten Ergebnisse stützen, um eine praxisnahe Umsetzung und praktikable Anwendung zu gewährleisten.

- **§23 Verwaltungsstrafbestimmungen**

Aufgrund der neuen Qualität des NISG und der damit verbundenen Meldepflichten ist es aus Sicht der FWAG im Sinn des Funktionierens des Systems förderlich, wenn vor einer allfälligen Geldstrafe zunächst Abhilfemaßnahmen seitens der Verwaltungsbehörde (z.B.: Bera-

tung, Aufforderungen zur Beseitigung der Verwaltungsübertretung, etc.) ergriffen werden, wenn diese eine Übertretung gemäß § 23 Abs. 1, 1.-6. feststellt.
Wie eingangs erwähnt liegt die Gewährleistung der Sicherheit von Netz- und Informationssystemen im ureigenen Interesse von Betreibern wesentlicher Dienste. Deshalb und aufgrund der gegenseitigen Vernetzung von BwD, Anbietern digitaler Dienste und Behörden haben alle Akteure ein Interesse am Funktionieren dieser Sicherheitsvorkehrungen. Ein sofortiges Strafen steht diesem gemeinsamen Interesse entgegen.
Zudem ist die Höhe der vorgesehenen Geldstrafen unverhältnismäßig hoch und sollten auf ***„bis zu 25.000 Euro, im Wiederholungsfall bis zu 50.000 Euro“*** halbiert werden.

Weitere Anmerkungen

- Das **Format für jene Meldungen**, die im Falle eines Sicherheitsvorfalls laut §16 von den Betreibern wesentlicher Dienste zu erfolgen haben, sollte standardisiert sein, um eine einheitliche Qualität der Meldungen zu gewährleisten. Am besten eignet sich dazu ein Web-Service, der für die BwD benutzerfreundlich gestaltet ist. Der (Zeit-) Aufwand für eine Meldung sollte jedenfalls so gering wie möglich gehalten werden, damit der BwD möglichst alle Ressourcen für die Behebung/Bearbeitung des Sicherheitsvorfalls verwenden kann.

- Um sich rechtzeitig für mögliche Cyberangriffe rüsten zu können, ist es geboten, etwaige **Angreiferinformationen** anderer Stellen bzw. anderer Unternehmen zugänglich machen. Das liegt sowohl im Interesse der einzelnen nicht-betroffenen Unternehmen/Stellen als auch im Sinn der gesamten Systemsicherheit.