Sehr geehrte Damen und Herren,

der ÖBB-Konzern stimmt dem Entwurf eines **Netz- und Informationssystemsicherheitsgesetzes** im Wesentlichen zu.

Wir übermitteln Ihnen nachstehend jedoch zwei Änderungsvorschläge mit der Bitte um entsprechende Berücksichtigung:

1) **NISG-BEGUT**_COO_2026_100_2_1555037, **§ 15 Abs. 3** „*Sicherheitsvorkehrungen für Betreiber wesentlicher Dienste*“ (Seite 9)

Aktuell:

(3) Die Betreiber wesentlicher Dienste haben mindestens alle drei Jahre die Erfüllung der Anforderungen nach Abs. 1 auf geeignete Weise gegenüber dem Bundesminister für Inneres nachzuweisen. Dieser Nachweis kann ein Jahr nach Zustellung des Bescheids gemäß § 14 Abs. 5 Z 1 jederzeit verlangt werden. Zu diesem Zweck übermitteln die Betreiber wesentlicher Dienste eine Aufstellung der vorhandenen Sicherheitsvorkehrungen durch den Nachweis von Zertifizierungen oder durchgeführten Überprüfungen durch qualifizierte Stellen (Abs. 4), einschließlich der dabei aufgedeckten Sicherheitsmängel. Der Bundesminister für Inneres kann zur Kontrolle der Einhaltung der Anforderungen nach Abs. 1 in die Netz- und Informationssysteme und diesbezügliche Unterlagen nehmen. Zur Herstellung der Anforderungen nach Abs. 1 ist der Bundesminister für Inneres ermächtigt, Empfehlungen auszusprechen, für deren Befolgung und entsprechenden Nachweis erforderlichenfalls eine angemessene Frist zu setzen ist, widrigenfalls die Befolgung bescheidmäßig angeordnet wird.

Vorschlag:

(3) Die Betreiber wesentlicher Dienste haben mindestens alle drei Jahre die Erfüllung der Anforderungen nach Abs. 1 auf geeignete Weise gegenüber dem Bundesminister für Inneres nachzuweisen. Dieser Nachweis kann ein Jahr nach Zustellung des Bescheids gemäß § 14 Abs. 5 Z 1 jederzeit verlangt werden. *Zu diesem Zweck übermitteln die Betreiber wesentlicher Dienste eine Aufstellung der vorhandenen Sicherheitsvorkehrungen, nach den Vorgaben der Sicherheitsvorkehrungsmaßnahmen des jeweiligen Sektors. Diese können durch den Nachweis von Zertifizierungen oder durchgeführten Überprüfungen durch qualifizierte Stellen (Abs. 4), einschließlich der dabei aufgedeckten Sicherheitsmängel, erbracht werden.* Der Bundesminister für Inneres kann zur Kontrolle der Einhaltung der Anforderungen nach Abs. 1 *Einschau, unter Beachtung geltender anderer Sicherheitsregeln wie Safetyanforderungen und anderen gesetzlichen Vorgaben,* in die Netz- und Informationssysteme und diesbezügliche Unterlagen nehmen. Zur Herstellung der Anforderungen nach Abs. 1 ist der Bundesminister für Inneres ermächtigt, Empfehlungen auszusprechen, für deren Befolgung und entsprechenden Nachweis erforderlichenfalls eine angemessene Frist zu setzen ist, widrigenfalls die Befolgung bescheidmäßig angeordnet wird.

2) **NISG-Erläuterungen**-COO_2026_100_2_1555053, **zu § 9** „*Befugnisse zur Vorbeugung von Sicherheitsvorfällen*“ (Seite 11):

Aktuell:

„Sinkholes“ hingegen sind insbesondere für die Erkennung von Botnetzen erforderlich, von denen eine wesentliche Gefahr für die Netz- und Informationssystemsicherheit in Österreich ausgeht. Ein Botnetz ist ein Zusammenschluss von netzwerkfähigen Geräten, die mit Schadsoftware infiziert sind und über einen oder mehrere sogenannte „C2-Server“ (Command and Control Server) kontrolliert und missbräuchlich verwendet werden können. „Sinkholes“ stellen Maßnahmen dar, die dahingehend Abhilfe schaffen, dass sie den Datenverkehr zwischen infizierten netzwerkfähigen Geräten und C2-Servern analysieren. Sie bieten somit die Möglichkeit, Botnetze entsprechend zu untersuchen und die Kommunikation zwischen infizierten Geräten und C2-Servern so einzuschränken, dass kein Schaden verursacht werden kann. Im Gegensatz zu „Honeypots“ werden „Sinkholes“ nur insofern genutzt, als der Bundesminister für Inneres „Sinkholes“ nicht von sich aus physisch betreibt, sondern nur auf den Datenverkehr von bei Betreibern wesentlicher Dienste, Anbietern digitaler Dienste und Einrichtungen des Bundes installierten Sinkholes Zugriff bekommt.

Vorschlag:

„Sinkholes“ hingegen sind insbesondere für die Erkennung von Botnetzen erforderlich, von denen eine wesentliche Gefahr für die Netz- und Informationssystemsicherheit in Österreich ausgeht. Ein Botnetz ist ein Zusammenschluss von netzwerkfähigen Geräten, die mit Schadsoftware infiziert sind und über einen oder mehrere sogenannte „C2-Server“ (Command and Control Server) kontrolliert und missbräuchlich verwendet werden können. „Sinkholes“ stellen Maßnahmen dar, die dahingehend Abhilfe schaffen, dass sie den Datenverkehr zwischen infizierten netzwerkfähigen Geräten und C2-Servern analysieren. Sie bieten somit die Möglichkeit, Botnetze entsprechend zu untersuchen und die Kommunikation zwischen infizierten Geräten und C2-Servern so einzuschränken, dass kein Schaden verursacht werden kann. Im Gegensatz zu „Honeypots“ werden „Sinkholes“ nur insofern genutzt, als der Bundesminister für Inneres „Sinkholes“ nicht von sich aus physisch betreibt, sondern nur auf den Datenverkehr von bei Betreibern wesentlicher Dienste, Anbietern digitaler Dienste und Einrichtungen des Bundes installierten Sinkholes Zugriff, *unter Beachtung geltender anderer Sicherheitsregeln wie Safetyanforderungen und anderen gesetzlichen Vorgaben,* bekommt.

Mit freundlichen Grüßen
Michael Krejci

Mag. Michael Krejci
Konzernrecht und Vorstandssekretariat

ÖBB-Holding AG
Unternehmenszentrale
Am Hauptbahnhof 2
1100 Wien
Tel. 01/93000/9744092
mobil 0664/6174998
Fax 01/93000/838/44092
mailto:michael.krejci@oebb.at
www.oebb.at

Österreichische Bundesbahnen-Holding Aktiengesellschaft, FN 247642f, Handelsgericht Wien, DVR 2111136, UID ATU58031338