**3266/AB**
**vom 02.11.2020 zu 3247/J (XXVII. GP)**

Bundesministerium
Finanzen

bmf.gv.at

**Mag. Gernot Blümel, MBA**
Bundesminister für Finanzen

Johannesgasse 5, 1010 Wien

Herrn Präsidenten
des Nationalrates
Mag. Wolfgang Sobotka
Parlament
1017 Wien

Geschäftszahl: 2020-0.561.963

Wien, 2. November 2020

Sehr geehrter Herr Präsident!

Auf die schriftliche parlamentarische Anfrage Nr. 3247/J vom 2. September 2020 der Abgeordneten Douglas Hoyos-Trauttmansdorff, Kolleginnen und Kollegen beehre ich mich Folgendes mitzuteilen:

Zu 1.:

Im Zuge der Nachbereitung des BMEIA-Cybervorfalles wurde unter Koordination des BKA ein strategisches Lessons Identified Dokument erstellt. Darin wurden kurz-, mittel- und langfristige Ziele zur Erhöhung der Widerstandsfähigkeit im Fall von Cybersicherheitsbedrohungen erarbeitet. Gleichzeitig haben sich die Prozesse gemäß NISG und Österreichische Strategie für Cybersicherheit (ÖSCS) 2013 in großen Teilen als zielgerichtet und effizient erwiesen. Die im Zuge des Lessons Identified festgestellten zweckmäßigen Verbesserungen werden im Wege der Novellierung des NISG als auch der Überarbeitung der ÖSCS adressiert werden. Grundsätzlich kann festgestellt werden, dass die Strukturen und Abläufe sowie die Zusammenarbeit der unterschiedlichen Stakeholder sehr gut funktionieren.

Weiters wird auf die angenommen Anträge NEOS und ÖVP/Grüne zur Cybersicherheit in der NSR-Sitzung vom 28. Februar 2020 sowie auf das Regierungsprogramm 2020 – 2024 der österreichischen Bundesregierung hingewiesen.

Wie schon in Beantwortung der schriftlichen parlamentarischen Anfrage Nr. 1309/J vom 25. März 2020 mitgeteilt, erfolgten basierend auf den Erkenntnissen und der Risikoeinschätzung des interministeriellen Krisenstabs direkte und konkrete Risikominimierungsmaßnahmen. Basierend auf den Erkenntnissen des Vorfalles wurden auch die jeweiligen Systeme gehärtet beziehungsweise die (automatisierten) Abwehrmaßnahmen verbessert.

Der Innere Kreis der operativen Koordinierungsstruktur beziehungsweise die Operative Koordinierungsstruktur (IKDOK/OPKOORD) erstellt regelmäßig basierend auf Meldungen gemäß dem NISG eigenen Systembeobachtungen und international zur Verfügung gestellten Daten sowohl eine Risikoeinschätzung als auch Empfehlungen zum Schutz der eigenen Systeme.

Zu 2.:

Die IKT-Sicherheit im Bund wird als fortlaufender Prozess verstanden. Dementsprechend werden, unterstützt durch das GovCERT und den IKDOK (Inneren Kreis der operativen Koordinierungsstruktur), kontinuierlich Anpassungen an der IKT-Sicherheitsstruktur vorgenommen. Dies betrifft sowohl die Beschaffung von State of the Art IKT-Sicherheitsinfrastruktur, als auch die permanente Evaluierung und Anpassung der Prozesse. Darüber hinaus werden basierend auf den aktuellen Bedrohungslagen bewusstseinsbildende Maßnahmen (Awareness) durchgeführt.

Zu 3.:

Wie schon in Beantwortung der schriftlichen parlamentarischen Anfrage Nr. 1309/J vom 25. März 2020 mitgeteilt, erfolgten basierend auf den Erkenntnissen und der Risikoeinschätzung des interministeriellen Krisenstabs direkte und konkrete Risikominimierungsmaßnahmen. Basierend auf den Erkenntnissen des Vorfalles wurden auch die jeweiligen Systeme gehärtet beziehungsweise die (automatisierten) Abwehrmaßnahmen verbessert.

Der Innere Kreis der operativen Koordinierungsstruktur beziehungsweise die Operative Koordinierungsstruktur (IKDOK/OPKOORD) erstellt regelmäßig basierend auf Meldungen

gemäß dem NISG eigenen Systembeobachtungen und international zur Verfügung gestellten Daten sowohl eine Risikoeinschätzung als auch Empfehlungen zum Schutz der eigenen Systeme.

Für das Bundesministerium für Finanzen hat der Schutz der verarbeiteten Daten eine hohe Priorität. Sowohl das Bundesministerium für Finanzen als auch die Bundesrechenzentrum GmbH (BRZ) verfügen über moderne Informationssicherheits-Managementsysteme, die nach dem internationalen Sicherheitsstandard ISO/IEC 27001 zertifiziert sind und jährlich überprüft werden. Die Managementsysteme des Bundesministeriums für Finanzen und der BRZ GmbH sorgen unter anderem dafür, dass bestehende Risiken systematisch identifiziert, beurteilt und mittels geeigneter Maßnahmen reduziert werden. Sie sehen darüber hinaus vor, dass die Wirksamkeit der Maßnahmen regelmäßig überprüft, bewertet und evaluiert wird.

Der öffentlich verfügbare Sicherheitsstandard ISO/IEC 27001 spezifiziert dafür einen umfassenden Katalog von Anforderungen beziehungsweise Maßnahmen, welche unter anderem auch den Bereich der Cybersicherheit betreffen. Im Hinblick auf die Effektivität dieser Maßnahmen ist es jedoch nicht möglich, die Maßnahmen sowie diesbezügliche Beschaffungen, Rahmenverträge und Kooperationspartner im Detail öffentlich mitzuteilen.

Zu 4. und 5.:

Wie schon in Beantwortung der schriftlichen parlamentarischen Anfrage Nr. 1309/J vom 25. März 2020 ausgeführt wurden im Zuge der Vorfallsbehandlung im BMEIA durch den Einsatzstab sowohl eine laufende Risikoeinschätzung als auch Empfehlungen für konkrete Absicherungen der eigenen Netze erstellt und kommuniziert. Diese Maßnahmen reichten beginnend von konkreten Scripts zum Scannen nach im BMEIA festgestellter Malware über das Einspielen von Indicators of Compromise (IOCs) in der eigenen Sicherheitsarchitektur bis hin zu Blacklists (Verweigerung zur Ausführung) von bestimmten Applikationen.

Die Aufwände und Kosten für diese Maßnahmen sind nur zum Teil dem Bereich IKT-Sicherheit zuordenbar und können daher nicht im Detail ausgewiesen werden.

Zu 6.:

Wie bereits in Beantwortung der schriftlichen parlamentarischen Anfrage Nr. 1309/J vom 25. März 2020 mitgeteilt, arbeiten die Mitarbeiterinnen und Mitarbeiter der IKT Sicherheit in einem sensiblen Bereich und müssen vor kriminellen Aktivitäten und nachrichtendienstlicher Ausspähung geschützt werden. Daher muss von einer konkreten Nennung von Anzahl und Namen Abstand genommen werden. Die Analysen und Verbesserungen der Sicherheit (Adaptierung bzw. Optimierung bestehender Systeme) erfolgen jedenfalls durch das im Zuge der Geschäfts- und Personaleinteilung eingeteilte Personal im Rahmen der routinemäßigen Aufgabenwahrnehmung.

Zu 7. und 8.:

Der Bund verfügt mit dem GovCERT und dem IKDOK über im NISG festgeschriebene Expertengruppen, auf welche sowohl in der routinemäßigen Risikoanalyse als auch im konkreten Anlassfall zugegriffen werden kann. Die Shared Services des Bundes in der BRZ (z.B. ELAK) unterliegen dem dort angesiedelten unternehmenseigenen CERT.

Der Bundesminister:
Mag. Gernot Blümel, MBA

Elektronisch gefertigt

| | | |
|---|---|---|
| BMF BUNDESMINISTERIUM FÜR FINANZEN | Prüfhinweis | Informationen zur Prüfung des elektronischen Siegels bzw. der elektronischen Signatur finden Sie unter: https://amtssignatur.brz.gv.at/ |
| | Datum/Zeit | 2020-11-02T10:13:43+01:00 |
| Unterzeichner | Bundesministerium für Finanzen | |
| Aussteller-Zertifikat | CN=a-sign-corporate-light-02,OU=a-sign-corporate-light-02,O=A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH,C=AT | |
| Serien-Nr. | 1814163722 | |
| Dokumentenhinweis | Dieses Dokument wurde amtssigniert. | |

| | | |
|---|---|---|
| REPUBLIK ÖSTERREICH Parlamentsdirektion SIEGEL | **Unterzeichner** | Parlamentsdirektion |
| | **Datum/Zeit-UTC** | 2020-11-02T10:19:14+01:00 |
| | **Prüfinformation** | Informationen zur Prüfung des elektronischen Siegels und des Ausdrucks finden Sie unter: https://www.parlament.gv.at/siegel |
| **Hinweis** | Dieses Dokument wurde elektronisch besiegelt. | |