

**11481/AB**  
Bundesministerium vom 08.09.2022 zu 11849/J (XXVII. GP)  
[bmf.gv.at](http://bmf.gv.at)  
Finanzen

**Dr. Magnus Brunner, LL.M.**  
Bundesminister für Finanzen

Herrn Präsidenten  
des Nationalrates  
Mag. Wolfgang Sobotka  
Parlament  
1017 Wien

Johannesgasse 5, 1010 Wien

Geschäftszahl: 2022-0.500.797

Wien, 8. September 2022

Sehr geehrter Herr Präsident!

Auf die schriftliche parlamentarische Anfrage Nr. 11849/J vom 8. Juli 2022 der Abgeordneten Rosa Ecker, MBA, Kolleginnen und Kollegen beehe ich mich Folgendes mitzuteilen:

Zu 1.:

Laut dem Computer Emergency Response Team (CERT) der Bundesrechenzentrum (BRZ) GmbH besteht im Zusammenhang mit Angriffen auf Grundlage des Modus Operandi, welcher beim Angriff auf das Amt der Kärntner Landesregierung zur Anwendung kam, für das Bundesministerium für Finanzen (BMF) derzeit kein Handlungsbedarf. Im Hinblick auf die Effektivität der diesbezüglich getroffenen Maßnahmen ist es jedoch nicht möglich, diese im Detail öffentlich mitzuteilen.

Zu 2.:

Es gab und gibt Versuche, Handlungen gemäß § 118a StGB gegen die Computersysteme des Ressorts zu setzen. Zum Schutz der Computersysteme werden spezifische Sicherheitsvorkehrungen eingesetzt. Im Hinblick auf die Effektivität dieser Maßnahmen ist es jedoch nicht möglich, diese im Detail öffentlich mitzuteilen.

### Zu 3., 5. und 6.:

Für das BMF hat der Schutz der verarbeiteten Daten und der dafür eingesetzten IT-Verfahren und IKT-Infrastrukturkomponenten eine hohe Priorität. Das BMF verfügt daher über ein kombiniertes Informationssicherheits- und Datenschutz-Managementsystem, das nach den internationalen Sicherheitsstandards ISO/IEC 27001 und ISO/IEC 27701 zertifiziert ist und jährlich überprüft wird. Das Managementsystem sorgt unter anderem dafür, dass die diesbezgl. geltenden Rechtsvorschriften eingehalten und bestehende Risiken systematisch identifiziert, beurteilt und mittels geeigneter Maßnahmen reduziert werden. Es sieht darüber hinaus vor, dass die Wirksamkeit der Maßnahmen sowohl regelmäßig als auch im Anlassfall überprüft, bewertet und evaluiert wird.

Die öffentlich verfügbaren Sicherheitsstandards ISO/IEC 27001 und ISO/IEC 27701 spezifizieren dafür umfassende Anforderungs- bzw. Maßnahmenkataloge. Im Hinblick auf die Effektivität dieser Maßnahmen ist es jedoch nicht möglich, diese im Detail öffentlich mitzuteilen.

### Zu 4. und 7.:

Es wird auf die Beantwortung der zu diesem Themenkreis auch an den Herrn Bundeskanzler ergangenen schriftlichen parlamentarischen Anfrage Nr. 11854/J vom 8. Juli 2022 verwiesen.

### Zu 8. und 9.:

Das BMF verfügt über einen Notfallplan, der die einzuleitenden Maßnahmen und Zuständigkeiten bei auftretenden Vorfällen im Zusammenhang mit wesentlichen Cyberbedrohungen regelt, und führt regelmäßige Notfallübungen in Form von Simulationen, Planspielen, Workshops und dergleichen durch. Das BMF hat in den letzten zehn Jahren an acht Übungen teilgenommen. Bei sieben davon handelte es sich um nationale oder internationale Übungen. Im Hinblick auf die Effektivität der diesbezüglich getroffenen Maßnahmen ist es jedoch nicht möglich, diese im Detail öffentlich mitzuteilen.

**Der Bundesminister:**  
**Dr. Magnus Brunner, LL.M.**

Elektronisch gefertigt

