8924/AB
vom 18.07.2016 zu 9311/J (XXV.GP)

REPUBLIK ÖSTERREICH
DER BUNDESMINISTER FÜR JUSTIZ

BMJ-Pr7000/0111-III 1/2016

Museumstraße 7
1070 Wien

Tel.: +43 1 52152 0
E-Mail: team.pr@bmj.gv.at

Frau
Präsidentin des Nationalrates

Zur Zahl 9311/J-NR/2016

Die Abgeordneten zum Nationalrat Rupert Doppler und weitere Abgeordnete haben an mich eine schriftliche Anfrage betreffend „Cyberkriminalität – Hackerangriffe auf Computersysteme des Bundes“ gerichtet.

Ich beantworte diese Anfrage aufgrund der mir vorliegenden Informationen wie folgt:

Zu 1:
Von Seiten des Bundesministeriums für Justiz und seines primären IT-Dienstleisters, der Bundesrechenzentrum GmbH (BRZG), wird eine Vielzahl von organisatorischen Maßnahmen gegen Cyberkriminalität sowie zur Gewährleistung eines verantwortungsvollen Umgangs mit Daten getroffen. Die Sicherheit von Daten ist dem Bundesministerium für Justiz naturgemäß ein zentrales Anliegen. „Cybersecurity“ ist Teil der Unternehmensstrategie der BRZG, die im Bereich Security auch über eine ISO 27001 Zertifizierung verfügt. Neben einem eigenen BRZG-internen Computer Emergency Response Team (BRZ-CERT) bestehen auch verschiedene Partnerschaften im Bereich Sicherheit (z.B. mit dem Computer Emergency Response Team Austria [CERT]). Die BRZG ist auch Mitglied im Kuratorium sicheres Österreich (KSÖ) sowie im Zentrum für sichere Informationstechnologie Austria (A-SIT).

Sämtliche Mitarbeiter/innen in der Justiz sowie in der BRZG werden hinsichtlich IT-Sicherheit geschult; zudem wird ein aktives, zeitnahes und abgestimmtes Informationsmanagement betrieben.

Daneben werden zahlreiche technische Vorkehrungen gegen Cyberkriminalität getroffen. Ich ersuche aber um Verständnis, dass es im Hinblick auf die Effektivität dieser Maßnahmen nicht tunlich ist, diese in einer öffentlichen Anfragebeantwortung näher darzulegen.

Zu 2 bis 7:
Der IT-technische Zentralknoten der Justiz in der BRZG ist regelmäßig Attacken ausgesetzt.

So finden z.B. „DDOS-Attacken“ und „Port-Scans“ nahezu täglich statt und werden sofort erkannt und abgewehrt. Auch besteht eine nahezu permanente Konfrontation mit „Standard SPAM“ und „Malware“ sowie - etwa monatlich - mit erweiterten Mailattacken auf eine größere Anzahl von Benutzern, wobei diese Angriffe zu 99,8 % abgewehrt werden können.

Ein nennenswerter Schaden ist durch Attacken bisher nicht entstanden. So kann insbesonders ausgeschlossen werden, dass durch die Attacken sensible Daten Dritten zugänglich gemacht wurden.

Ergänzend weise ich darauf hin, dass die einzelnen Justizdienststellen über keinen separaten Internetzugang verfügen und spezifische (Hack)Angriffe auf einzelne Dienststellen bisher nicht stattfanden.

Eine detailliertere Antwort kann aber auch hier im Hinblick auf die Effektivität der Abwehrmaßnahmen nicht gegeben werden, wofür ich um Verständnis ersuche.

Zu 8:
An tatsächlichen Ausgaben entstehen der Justiz gegenüber der BRZG für IT-Sicherheit jährliche Kosten in Höhe von rund 800.000 Euro. Die justizintern anfallenden Kosten durch den Einsatz von Justizmitarbeiterinnen und Justizmitarbeitern (IT-Administration, Mitarbeiterschulungen usw.) werden nicht gesondert erfasst und können daher nicht beziffert werden.

Wien, 18. Juli 2016

Dr. Wolfgang Brandstetter

REPUBLIK ÖSTERREICH JUSTIZ SIGNATUR	**Datum/Zeit**	2016-07-18T10:30:26+02:00
	Hinweis	Dieses Dokument wurde elektronisch signiert. Auch ein Ausdruck dieses Dokuments hat die Beweiskraft einer öffentlichen Urkunde.
	Prüfinformation	Informationen zur Prüfung des elektronischen Siegels bzw. der elektronischen Signatur und des Ausdrucks finden Sie unter: http://kundmachungen.justiz.gv.at/justizsignatur

REPUBLIK ÖSTERREICH Parlamentsdirektion SIEGEL	**Unterzeichner**	Parlamentsdirektion
	Datum/Zeit-UTC	2016-07-18T10:33:20+02:00
	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.	