13.34

Bundesminister für Europa, Integration und Äußeres Mag. Alexander Schallenberg, LL.M.: Sehr geehrte Damen und Herren! Hohes Haus! Es war mir ein persönliches Anliegen, diese Gelegenheit zu nützen, um Sie heute über den aktuellen Stand des laufenden Angriffs auf das IT-System des Außenministeriums zu informieren. Es handelt sich nämlich tatsächlich um einen massiven Angriff auf unser IT-System. Leider sind ja solche Attacken, die sich manchmal auch über längere Zeiträume hinweg ziehen können, heutzutage nichts Ungewöhnliches mehr. Mehrere andere Mitgliedstaaten waren bereits mit ähnlichen Angriffen konfrontiert und auch nicht staatliche Einrichtungen und Firmen sind davor nicht gefeit und regelmäßig Gegenstand solcher Vorfälle.

Nach unserem heutigen Wissensstand handelt es sich bei diesem laufenden Angriff um eine gezielte Cyberattacke gegen das Außenministerium mit dem Ziel der Informationsbeschaffung.

Mir ist es dabei wichtig, gleich zu Beginn zwei wesentliche Punkte klarzustellen:

Erstens: Es konnte bis jetzt kein Abfluss von Informationen aus dem Außenministerium festgestellt werden.

Zweitens: Zu keinem Zeitpunkt war die Funktionsfähigkeit unserer weltweiten konsularischen Dienstleistungen gefährdet.

Das heißt, die Services des Außenministeriums für die Bürgerinnen und Bürger – sei es an den Botschaften und Konsulaten, sei es auf der Homepage, sei es via Mail oder in den verschiedenen Apps auf den Handys – waren und sind sicher.

Ich kann Ihnen, sehr geehrte Damen und Herren Abgeordnete, heute folgenden Überblick über das bisherige Geschehen geben: Am 3. Januar ist der Angriff auf das interne IT-System des Außenministeriums bekannt geworden. Oft laufen solche Angriffe ja zum Teil tage-, wochen- oder sogar monatelang unbemerkt, bevor man überhaupt draufkommt. In diesem Fall hatten wir aber das Glück, dass das IT-Team des Außenministeriums binnen weniger Tage diesen Angriff erkannt und umgehend Gegenmaßnahmen eingeleitet hat. Seit Bekanntwerden der Angriffe arbeitet ein großes Team aus mehreren Dutzend Expertinnen und Experten rund um die Uhr und mit Hochdruck daran, diesen Angriff abzuwehren und die volle Datensicherheit wiederherzustellen.

Dabei steht das Außenministerium aber nicht alleine da. Von Anfang an arbeiteten die Fachleute aus meinem Haus mit den Expertinnen und Experten des Innenministeriums, der Landesverteidigung sowie des Bundeskanzleramtes engstens zusammen, wobei wir

auch externe Experten hinzugezogen haben. Dieses ministeriumsübergreifende Team arbeitet nun seit über zwei Wochen rund um die Uhr, muss man sagen, und unermüdlich an der Lösung der Situation. Ich konnte mich auch selbst davon überzeugen, wie gut diese Zusammenarbeit zwischen den Bundesstellen funktioniert.

Erlauben Sie mir daher, dass ich an dieser Stelle nicht nur den Expertinnen und Experten aus meinem Haus, sondern vor allem auch den Mitarbeiterinnen und Mitarbeitern aller involvierten Dienststellen, insbesondere des Innenministeriums, des Verteidigungsministeriums und des Bundeskanzleramtes, meinen ganz herzlichen Dank für die wirklich beeindruckende Arbeit und den großen Einsatz, den sie hier zeigen, aussprechе. *(Beifall bei ÖVP und Grünen.)*

Gerade in diesem Fall zeigt es sich wieder, dass Sicherheit eben doch eine Querschnittsmaterie ist – Sicherheit betrifft uns alle – und dass gerade in unserer digitalisierten Welt eine enge Kooperation bei der Abwehr von Cyberattacken einfach unerlässlich ist. Für dieses vernetzte Vorgehen gibt uns das Netz- und Informationssystemsicherheitsgesetz den Rahmen vor. Ein interministerieller Koordinationsausschuss wurde zur Beratung über die operativen Maßnahmen zur Bewältigung des Vorfalls eingerichtet. Ein Technikerstab wurde gebildet, der von unterschiedlichen Ministerien beschickt wird. Da auch die Daten der Mitarbeiterinnen und Mitarbeiter des Außenministeriums von diesem Vorfall betroffen sein können, wurden sie entsprechend den Bestimmungen des Datenschutzgesetzes über den Vorfall informiert, damit sie selber entsprechende Vorsichtsmaßnahmen treffen können. Ebenso wurde sicherheitshalber auch die Datenschutzbehörde eingeschaltet.

Selbstverständlich haben wir auch die europäische Ebene eingeschaltet. Auf Ebene der Europäischen Union wurde der Vorfall umgehend dem EU Rapid Alert System gemeldet. Es versteht sich eigentlich von selbst, dass wir bei diesem Vorfall – und bei einem Vorfall dieser Größe selbstverständlich – auch eng mit unseren EU-Partnern zusammenarbeiten. Ich möchte mich daher an dieser Stelle ausdrücklich für die große Unterstützung bedanken, die wir von anderen Mitgliedstaaten bei diesem Vorfall erhalten haben. *(Beifall bei ÖVP und Grünen.)*

Unsere Expertinnen und Experten arbeiten dabei nicht nur daran, den unmittelbaren Angriff abzuwehren und einzudämmen, sie arbeiten natürlich auch daran, Klarheit über die Hintergründe und die Herkunft des Angriffs zu kriegen. Derzeit, das muss ich ganz offen sagen, liegen aber noch nicht genügend greifbare Anhaltspunkte vor, um klar in eine Richtung zeigen zu können, um völlig zweifelsfrei und klar von einer Urheberschaft zu sprechen.

Mitte Februar wird sich hier im Hohen Haus der Ständige Unterausschuss des Innenausschusses mit dieser Cyberattacke befassen. Dort werden Innenminister Karl Nehammer und ich selbst die jüngsten Entwicklungen darstellen, die neuesten Informationen mit Ihnen teilen und weitere Aspekte dieses Vorfalls erörtern. Ich ersuche Sie aber um Verständnis, dass ich aus technischen und vor allem aus ermittlungstaktischen Gründen derzeit keine weiteren Details bekannt geben kann.

Lassen Sie mich abschließend noch Folgendes klarstellen: Die Löscharbeiten laufen sehr intensiv und hochprofessionell, aber noch können wir nicht Brand gelöscht melden. Die staatlichen Sicherheitsnetzwerke haben sich insgesamt bewährt. Nach der raschen Entdeckung des Angriffs arbeiten die Expertinnen und Experten nun mit Hochdruck an der Eindämmung der Folgen.

Drittens, und das ist mir sehr wichtig: Die Services, die Dienstleistungen des Außenministeriums für die Bürgerinnen und Bürger, von der Ausstellung von Notpässen bei den Konsulaten und Botschaften bis zu den Reisewarnungen auf unserer Homepage, waren zu jedem Zeitpunkt gesichert. *(Beifall bei der ÖVP und bei Abgeordneten der Grünen.)*

Wir gehen aber im vorliegenden Fall auch über das unmittelbare Krisenmanagement hinaus. Wir nützen diesen Vorfall auch, um wichtige Lehren für die künftige Sicherheitsarchitektur aller Bundesstellen zu gewinnen. Heute ist das Außenministerium betroffen, aber es gilt, die richtigen Schlüsse zu ziehen, um künftig alle Bundeseinrichtungen noch besser schützen zu können.

Die in den letzten Tagen und Wochen gewonnenen Erfahrungen liefern uns dabei wichtige Erkenntnisse. Sie erlauben es, Verbesserungen für die IT-Sicherheit und das IT-Krisenmanagement des gesamten Bundesdienstes vorzunehmen, um sicherzustellen, dass stets alle Dienstleistungen der öffentlichen Hand auf IT-Ebene, die die Bürgerinnen und Bürger völlig zu Recht erwarten und von uns verlangen, immer zur Verfügung stehen und auch künftig wirklich gesichert sind. – Ich danke Ihnen für Ihre Aufmerksamkeit. *(Beifall bei ÖVP und Grünen.)*

13.41

Präsidentin Doris Bures: Danke, Herr Bundesminister.

Wir gehen gleich in die Debatte über die Erklärung ein.

Zu Wort gelangt Herr Abgeordneter Reinhold Einwallner. – Bitte.