Bericht der Untersuchungs-kommission

„Sicherheit und Prozesse“

Wien, Oktober 2025

Inhalt

I. Einleitung **3**

II. Ergebnisse **5**

1. Disziplinarverfahren, Dienstrecht und damit in Zusammenhang stehende Prozesse im BMEIA 5

a. Ergebnis der Erhebungen 5

b. Bewertung durch die Untersuchungskommission 7

c. Empfehlungen 11

2. Sicherheit der IKT-Systeme des BMEIA 14

a. Ergebnis der Erhebungen 14

b. Bewertung durch die Untersuchungskommission 15

c. Empfehlungen 17

3. Möglichkeit der Einflussnahme auf den betroffenen Beamten 18

a. Ergebnis der Erhebungen 18

b. Bewertung durch die Untersuchungskommission und Empfehlungen 19

I. Einleitung

Am Samstag, dem 26. Juli 2025, berichteten Medien erstmals über das mögliche Fehlverhalten eines leitenden Beamten einer österreichischen Vertretungsbehörde im Ausland. Dabei wurden die Vorwürfe unter anderem in den Kontext vergangener Angriffe auf die Integrität der IKT-Infrastruktur des Bundesministeriums für europäische und internationale Angelegenheiten (BMEIA) gestellt. Die öffentliche Berichterstattung warf Fragen zu potenziellen Sicherheitslücken im BMEIA sowie zu den internen Prozessen in diesem Zusammenhang auf.

Aus diesem Grund setzte Bundesministerin Mag. Beate Meinl-Reisinger, MES am 14. August 2025 eine unabhängige, multidisziplinäre Untersuchungskommission gemäß § 8 BMG ein. Deren Erhebungsauftrag umfasste die Überprüfung organisatorischer und sicherheitsrelevanter Aspekte sowie die Erarbeitung von Empfehlungen zur Verbesserung der internen Prozesse und Sicherheitsvorkehrungen im BMEIA.

Die Kommission setzte sich wie folgt zusammen:

- Bundesminister a.D. Mag. Thomas Starlinger (Vorsitz)
- Georg Beham, MSc
- Mag. Helga Berger
- Mag. Otmar Lendl
- MMag. Dr. Elisabeth Tichy-Fisslberger (ab 12. September 2025)

Die Kommission konstituierte sich am 28. August 2025 und nahm sodann ihre Erhebungstätigkeit auf.

Bundesministerin Meinl-Reisinger hatte das BMEIA im Rahmen der Einsetzung der Kommission angewiesen, diese bei der Erfüllung ihrer Aufgaben uneingeschränkt zu unterstützen, insbesondere durch Akteneinsicht und die Erteilung von Auskünften auf Verlangen. Zur administrativen Unterstützung der Kommission wurde eine Geschäftsstelle eingerichtet, die aus zwei Bediensteten des BMEIA bestand.

Anlässlich ihrer Tätigkeitsaufnahme wurden die Kommissionsmitglieder nachweislich dazu verpflichtet, die geltenden gesetzlichen Regelungen – einschließlich der Verschwiegenheitspflichten gemäß dem Informationssicherheitsgesetz – zu beachten und einzuhalten.

Die Erhebungen der Kommission erfolgten auf Grundlage der folgenden Informationsquellen:

- Gespräche von Kommissionsmitgliedern mit Auskunftspersonen;
- Aktenstudium;
- Auswertung der medialen Berichterstattung;
- Best-Practice-Modelle und Standards anderer Behörden.

Die multidisziplinäre Zusammensetzung der Kommission erwies sich als besonders wertvoll, da sie eine adäquate Abbildung juristischer Aspekte, der Spezifika des auswärtigen Dienstes sowie von Fragen der IT-Sicherheit in der Berichtslegung ermöglichte.

Auf Einladung wurden durch die Kommission Gespräche mit 16 Auskunftspersonen im In- und Ausland auf freiwilliger Basis geführt. Die Möglichkeit das Gespräch mit der Kommission eigeninitiativ zu suchen, wurde nicht wahrgenommen. Die Gespräche mit den Auskunftspersonen fanden fast ausschließlich persönlich statt, vereinzelt im Plenarformat, meist durch zwei Kommissionsmitglieder (Vier-Augen-Prinzip). In einem Fall wurde das Gespräch ausnahmsweise über eine gesicherte Videokonferenzplattform abgehalten. Die Gespräche dauerten im Durchschnitt ein bis zwei Stunden und waren durchwegs von einem substanziellen und konstruktiven Dialog geprägt.

Die auf Ersuchen der Kommission zielgerichtet angeforderten Akten wurden von den jeweils besonders qualifizierten Kommissionsmitgliedern themenspezifisch analysiert, in den weiteren Kontext des Untersuchungsgegenstandes eingeordnet und in weiterer Folge der gesamten Kommission zur Verfügung gestellt.

Im Austausch mit Sicherheitsbehörden wurden zudem deren Erfahrungswerte und Praxis abgefragt. Dieser Input soll dazu beitragen, zukünftige Prozesse im BMEIA effizienter, effektiver und nachvollziehbarer zu gestalten.

Die auf IKT und Cybersicherheit bezogenen Aspekte der Untersuchung folgten methodisch den Prinzipien einschlägiger Auditverfahren unter Berücksichtigung internationaler Standards und des Stands der Technik.

Festzuhalten ist, dass sich die Kommission weder als Ersatz für ressortinterne Kontrollmechanismen noch als Einrichtung zur nachträglichen Revision früherer Entscheidungen verstanden hat. Ihr Ziel war es vielmehr, entsprechend den Vorgaben von Bundesministerin Meinl-Reisinger, aus Erkenntnissen der Vergangenheit Ableitungen für in Zukunft verbesserte Prozesse im BMEIA zu erarbeiten – nicht zuletzt angesichts immer komplexerer Herausforderungen für staatliche Institutionen.

Die Kommissionsmitglieder haben ihre Erkenntnisse, Bewertungen und Empfehlungen während des gesamten Prozesses miteinander geteilt und in der Erstellungsphase des Berichts intensiv diskutiert, um eine größtmögliche Objektivität und Nachvollziehbarkeit zu gewährleisten. Der vorliegende Bericht wurde – so wie alle Entscheidungen des Gremiums – im Konsens angenommen.

Zum Schutz der Persönlichkeitsrechte einzelner Bediensteter wurde in der Berichtslegung zum Teil auf abstrakte Beschreibungen zurückgegriffen.

II. Ergebnisse

1. Disziplinarverfahren, Dienstrecht und damit in Zusammenhang stehende Prozesse im BMEIA

a. Ergebnis der Erhebungen

Am 16. und 17. September 2024 langten im Generalinspektorat des BMEIA *(Anm.: innere Revision des Ressorts)*, das im Bereich des BMEIA als Kontaktstelle für Meldungen nach dem HinweisgeberInnenschutzgesetz (HSchG) fungiert, Hinweise ein, in denen drei Sachverhalte betreffend einen leitenden Beamten einer österreichischen Vertretungsbehörde im Ausland dargelegt wurden. Es handelte sich dabei um die ersten Meldungen, die von der Bundesdisziplinarbehörde in deren Eigenschaft als zentraler Meldestelle für Hinweise nach dem HSchG an das BMEIA übermittelt wurden. Die Sachverhalte samt Unterlagen wurden auf der „BRZ Gover Drive“ zur Verfügung gestellt und konnten mittels Link abgerufen werden. Nach Rücksprache mit dem Generalsekretär des BMEIA über die zu verfolgende Vorgehensweise bei HSchG-Eingaben leitete die Leiterin des Generalinspektorats die Hinweise am 20. September 2024 an die Leiterin der Sektion VI (Management) zur Prüfung und allfälligen Einleitung weiterer Maßnahmen weiter.

Die Leiterin der Sektion VI beauftragte in der Folge den Leiter der Abteilung VI.1 (Personalangelegenheiten) in dessen Eigenschaft als Vertreter der Dienstbehörde, gemeinsam mit dem der Sektion VI zugeordneten Fachexperten für Dienst-, Besoldungs- und Disziplinarrecht, mit der Prüfung und Beurteilung folgender in den Hinweisen enthaltener drei Sachverhalte:

1. die behauptete ungebührliche Einflussnahme des betroffenen Beamten auf eine Dienstprüfung durch Hilfestellung für die zu prüfende Person;
2. die behauptete, angesichts der fachlichen und persönlichen Qualifikation ungerechtfertigte, unangebrachte bzw. rechtswidrige Anstellung einer Kabinettsmitarbeiterin im BMEIA im Jahr 2021; und
3. den behaupteten Betrieb eines pornografischen Blogs von 2014 bis März 2024 mit Fotos und vermeintlich rassistischen, frauenfeindlichen und gewaltbeschreibenden Texten durch den betroffenen Beamten, zum Teil während der Dienstzeit und unter Verwendung von Dienstgeräten, eine vermeintliche Verbindung zwischen dem Betrieb dieses Blogs und dem Cyberangriff auf das BMEIA im Jahr 2020 sowie die behauptete Nicht-Beachtung von Hinweisen auf diese Tätigkeit durch zuständige Stellen im BMEIA.

Die Dienstbehörde prüfte diese Sachverhalte auf Grundlage der beigelegten Beweisfotos, von relevanten Akten der Personalabteilung, eines Gesprächs mit dem betroffenen Beamten am 9. Oktober 2024 und zwei von diesem übermittelten schriftlichen Stellungnahmen vom 15. und 21. Oktober 2024 und veranlasste eine technische Analyse durch die Abteilung VI.7 (IKT). Weitere Abteilungen des BMEIA (insbesondere die Abteilung für Sicherheitsangelegenheiten) wurden in die Erhebung der Entscheidungs-

grundlagen nicht einbezogen. Der betroffene Beamte wurde außerdem am 11. November 2024 durch den Abteilungsleiter VI.1 zum Ergebnis der technischen Analyse befragt.

Der Fachexperte für Dienst-, Besoldungs- und Disziplinarrecht erstellte eine Zusammenfassung der rechtlichen Rahmenbedingungen zur Beurteilung der Sachverhalte aus disziplinarrechtlicher, dienstrechtlicher und strafrechtlicher Sicht, die am 8. Oktober 2024 erstmals mit dem Abteilungsleiter VI.1 besprochen wurde. Auf Grundlage dieser Erhebungen erstellte die Dienstbehörde eine schriftliche Darstellung des Sachverhalts (gezeichnet mit Datum 28. November 2024), der Prüfung der Vorwürfe durch die Dienstbehörde und des rechtlichen Rahmens samt Empfehlung einer disziplinären Maßnahme. Diese Darstellung der Dienstbehörde wurde an die weisungsbefugten Stellen des Ressorts gerichtet und in weiterer Folge, laut übereinstimmenden Aussagen von Auskunftspersonen, mit diesen Stellen mündlich erörtert. Ein schriftlicher Austausch mit diesen Stellen konnte auf Basis des vorgelegten Schriftguts weder festgestellt noch ausgeschlossen werden.

Am 13. Dezember 2024 wurde darüber hinaus der Dienststellenausschuss des BMEIA gem. § 9 Abs. 3 lit. c Personalvertretungsgesetz über die beabsichtigte Verhängung der Disziplinarstrafe informiert. Nach übereinstimmenden Aussagen von Auskunftspersonen hatte dieser in weiterer Folge einstimmig eine Abberufung des betroffenen Beamten empfohlen.

Die Dienstbehörde verneinte eine strafrechtliche Relevanz, eine Befassung der Justizbehörden gemäß § 78 Strafprozessordnung wurde nicht im Detail geprüft. Am 18. Dezember 2024 wurde gegen den betroffenen Beamten eine Disziplinarstrafe in Form eines Verweises gemäß § 92 Abs. 1 Z 1 BDG 1979 erlassen. Als Ergebnis der Erhebungen der Dienstbehörde lagen dem Verweis als nachgewiesener Sachverhalt der Betrieb des oben beschriebenen Blogs (*Anmerkung:* gemäß damaliger Aktenlage jedoch außerhalb der Dienstzeiten und nicht von dienstlichen Geräten aus) und der einmalige Versuch der Verfälschung eines Dienstprüfungsergebnisses durch Hilfestellung zugunsten einer Prüfungskandidatin durch den betroffenen Beamten in seiner Eigenschaft als Mitglied der Dienstprüfungskommission des BMEIA zu Grunde. Dementsprechend wurden Dienstpflichtverletzungen gemäß § 43 Abs. 1 und 2 BDG 1979 festgestellt. Im Hinblick auf den oben unter Punkt 2. dargestellten Sachverhalt wurde im Zuge der Erhebungen kein Fehlverhalten des betroffenen Beamten festgestellt.

Am 19. Dezember 2024 gab der betroffene Beamte eine schriftliche Erklärung ab, wonach er derartige oder vergleichbare Handlungen und Verhaltensweisen in der Zukunft keinesfalls wieder setzen und generell alles unterlassen werde, was geeignet wäre, das Vertrauen der Allgemeinheit in die sachliche Wahrnehmung seiner Aufgaben zu erschüttern sowie auch all seinen Dienstpflichten umfassend, zuverlässig und treu nachzukommen.

Ebenfalls am 19. Dezember 2024 informierte die Dienstbehörde das Generalinspektorat über die von ihr in Folge der eingelangten Hinweise gesetzten Schritte. Der Leiter des Generalinspektorats gab der Bundesdisziplinarbehörde als Meldestelle nach dem HSchG am 7. Jänner 2025 die gesetzten Maßnahmen bekannt. Der Verweis wurde dem Disziplinaranwalt im BMEIA erst am 13. August 2025 zugestellt.

Von einer Abberufung vom Arbeitsplatz und Einberufung des betroffenen Beamten in die Zentrale wurde zum damaligen Zeitpunkt abgesehen.

Am 26. Juli 2025 berichtete ein österreichisches Online-Medium unter dem Titel „Sadomaso im Außenministerium“ erstmals über den Fall. Es folgte weitere Berichterstattung in österreichischen und internationalen Medien, wodurch der Sachverhalt eine breite Aufmerksamkeit erlangte.

In Folge dieser Medienberichterstattung bot der betroffene Beamte Außenministerin Meinl-Reisinger seine Abberufung an, die am 30. Juli 2025 zu dessen Abberufung führte.

b. Bewertung durch die Untersuchungskommission

i. Zum Prozess betreffend Meldungen nach dem HinweisgeberInnenschutzgesetz (HSchG):

Es fehlte im BMEIA zum Zeitpunkt des Einlangens der Meldungen nach dem HSchG im Anlassfall an einer festgelegten Vorgehensweise für die Behandlung von solchen Hinweisen durch das Generalinspektorat. Im Anlassfall musste die Generalinspektorin daher mit dem Generalsekretär als ihrem Vorgesetztem ad hoc Rücksprache halten, um das weitere Prozedere zu definieren. Zwar ist aus Sicht der Kommission an dem weiteren Vorgehen im Anlassfall im Hinblick auf die Umsetzung des HSchG nichts auszusetzen, jedoch wäre im Sinne einer unvoreingenommenen, unbefangenen Behandlung ein im Vorhinein festgelegter Prozess samt Vorgaben geboten.

Im Hinblick auf die Rolle des Generalinspektorats im Zusammenhang mit Meldungen nach dem HSchG besteht darüber hinaus Klarstellungsbedarf. Dessen Tätigwerden („Objektive Prüfungs-, Kontroll- und Beratungsleistungen […] zur Sicherstellung der Gesetzmäßigkeit und Ordnungsmäßigkeit der Verwaltung sowie einer sparsamen und zweckmäßigen Gebarung im Wirkungsbereich des Bundesministeriums und aller ihm nachgeordneter Dienststellen“) beruht auf der „Revisionsordnung für das Bundesministerium für europäische und internationale Angelegenheiten“ aus dem Jahr 2011. Es ist fraglich, ob diese Verwaltungsverordnung auch auf die geschäftseinteilungsmäßige Funktion als „Kontaktstelle der Bundesdisziplinarbehörde für Meldungen nach dem HinweisgeberInnenschutzgesetz (HSchG) im Bereich des BMEIA“ Anwendung findet. Bejahendenfalls wäre eine genaue schriftlich nachweisbare Information des vorgesetzten Generalsekretärs im Anlassfall angezeigt gewesen. Bei Verneinung der Anwendbarkeit der Revisionsordnung wäre die Vorgangsweise der Generalinspektorin, sich auf die Funktion eines „Briefkastens“ für Bundesdisziplinarbehörde und Dienstbehörde zu beschränken, nachvollziehbar. Nach derzeitigem Stand ist das Generalinspektorat jedenfalls nicht verpflichtet, abschließend zu prüfen, ob dem gemäß HSchG erfolgten Hinweis entsprechend nachgegangen wurde.

ii. Zum Prozess betreffend Disziplinarverfahren:

Das BMEIA ist hinsichtlich seines Personalstands im Vergleich zu anderen Bundesministerien ein „kleines“ Ressort. Dementsprechend kommt es zu einer geringeren Anzahl an Disziplinarverfahren als in deutlich größeren Ressorts, sodass weniger Erfahrung und praktische Kenntnis aufgebaut werden

können. Im Zeitraum von 2020 bis zum Ende der Erhebungen der Kommission kam es zu 13 Disziplinarverfahren.

Die Untersuchung hat gezeigt, dass bei Bekanntwerden mutmaßlicher Dienstpflichtverletzungen im BMEIA nicht nach einem einheitlichen Standardprozess vorgegangen wird. Dies betrifft insbesondere die fehlende aktenmäßige Befassung einzelner Stellen, wie etwa der Sicherheitsabteilung, die Dokumentation und die Entscheidungsvorbereitung. In Bezug auf die Nachvollziehbarkeit, Objektivität und Kontinuität dieser Verfahren erscheint dies in vielerlei Hinsicht problematisch, was sich auch im Anlassfall manifestiert hat. Eine Problematik, die sich bei Disziplinarverfahren in kleineren Ressorts, nicht nur speziell im BMEIA stellt, ist die hohe Wahrscheinlichkeit, dass die in der Dienstbehörde handelnden Personen eine persönliche Beziehung zu der Person haben, auf die sich das Verfahren bezieht. Auch diesbezüglich fehlt es im BMEIA an Vorgaben zur Meldung von Befangenheiten im Sinn des § 7 Abs. 1 Allgemeines Verwaltungsverfahrensgesetz 1991.

Die Tatsache, dass die Bearbeitung der über die Meldestelle nach dem HSchG eingelangten Hinweise im Anlassfall ausschließlich der Abteilung für Personalangelegenheiten oblag, führte zu einer entsprechend eingeschränkten Betrachtung. So wurden in letzter Konsequenz sicherheitsrelevante und außenpolitische Elemente unzureichend beachtet, ermittelt und in die Entscheidung über die Disziplinarverfügung einbezogen. Dies betraf beispielsweise den Aspekt der Erpressbarkeit des Beamten etwa durch externe Akteure im Zusammenhang mit dessen nachgewiesener Dienstpflichtverletzung (Betreiben des pornografischen Blogs). Ebenso wenig wurde die Vertrauenswürdigkeit gemäß § 55 Sicherheitspolizeigesetz des betroffenen Beamten in Zweifel gezogen. Nach Einschätzung der Kommission ist dies vor allem auf die mangelnde Befassung der Abteilung I.2 (Sicherheitsangelegenheiten) zurückzuführen. In Kenntnis der Fakten hätte diese eine erneute Sicherheitsüberprüfung der betroffenen Person veranlassen können bzw. müssen; zudem wäre eine zeitnahe forensische Untersuchung der dienstlich genutzten IKT-Geräte angezeigt gewesen.

Festzuhalten ist, dass zum Zeitpunkt des Disziplinarverfahrens nicht der gesamte Inhalt des Blogs bekannt war. Laut Aktenlage war dieser auf der Blog-Plattform bereits gelöscht worden. Dem betreffenden Hinweis waren 32 Fotos angefügt, die Ausschnitte aus dem Blog zeigten. Im Rahmen der verfügbaren technischen Mittel und rechtlichen Vorgaben konnte die von der Dienstbehörde befasste Abteilung VI.7 (IKT) den Blog nach eigenen Angaben nicht rekonstruieren, da in einer IKT-Abteilung hierfür die erforderliche tiefgehende forensische Expertise und die Werkzeuge fehlen. Eine Einbindung externer fachkundiger Stellen – etwa im Wege der Amtshilfe – hätte voraussichtlich Abhilfe für die Erhebungen im Disziplinarverfahren schaffen können, insbesondere durch die Wiederherstellung historischer Webseitenstände, und eine Chance eröffnet, diesen Blog aus allen öffentlich einsehbaren Webarchiven noch vor dessen Veröffentlichung durch Medien löschen zu können.

Das Aktenstudium durch die Kommission und die dazu geführten Gespräche haben gezeigt, dass einzelne Erhebungen und Feststellungen in Disziplinarverfahren durch die Dienstbehörde zum Teil unzureichend dokumentiert werden. So wurden etwa im Anlassfall nicht alle den eingelangten Hinweisen beigefügten Unterlagen in elektronischer Form im Akt gesichert, die Download-Links sind jedoch

mittlerweile abgelaufen. Ein weiteres Beispiel unzureichender Dokumentation des Anlassfalls ist, dass die technische Analyse der IKT-Abteilung in einem zusammenfassenden Sachverhalt erwähnt und deren Ergebnisse der Disziplinarverfügung zu Grunde gelegt wurden, jedoch sind weder der Auftrag noch das Ergebnis durch E-Mails oder andere Dokumente der IKT-Abteilung im Akt belegt. Auch die Gespräche mit Mitgliedern der Personalvertretung und allfällige Empfehlungen des Dienststellenausschusses wurden durch die Dienstbehörde nicht schriftlich dokumentiert.

Die Kommission hat festgestellt, dass bei der Behandlung und Entscheidung von Disziplinarfällen im BMEIA die Genehmigung des betreffenden Akts durch die Leitung der Abt. VI.1 erfolgt. Die Sektionsleitung wird in den Aktenläufen lediglich „zur Stellungnahme“ oder „zur Information“ befasst. Eine Einbindung des Büros des Generalsekretärs bzw. des Generalsekretärs ist im Prozesslauf derzeit nicht zwingend vorgesehen, selbst dann nicht, wenn es um hochrangige Bedienstete geht. Eine solche fand nur vereinzelt, ohne erkennbares Muster, statt. Dies erweckt den Eindruck, dass die Entscheidungen in Disziplinarverfahren und die Verantwortlichkeit hierfür ausschließlich in der Abteilung VI.1 liegen. Zumindest im Anlassfall entspricht dies jedoch nicht den Wahrnehmungen der Kommission und trägt auch generell der Bedeutung gewisser Fälle nicht Rechnung.

Im Anlassfall ergibt sich aus der bereits erwähnten schriftlichen Darstellung, dass die Dienstbehörde empfohlen hatte, dem betroffenen Beamten eine disziplinäre Maßnahme in Form eines Verweises gemäß § 92 Abs. 1 Z 1 BDG 1979 zu erteilen. Die laut übereinstimmenden Aussagen von Auskunftspersonen daraufhin erfolgten Besprechungen mit den weisungsbefugten Stellen des Ressorts über die Frage, ob ein abgekürztes Verfahren gemäß § 131 BDG gewählt bzw. welche Disziplinarstrafe verhängt werden soll, sind im Akt nicht dokumentiert. Es lässt sich aktenmäßig nicht nachvollziehen, weshalb keine Disziplinaranzeige an die Bundesdisziplinarbehörde erstattet wurde, wer *de facto* über die konkrete Disziplinarstrafe befunden hat und wie die Strafbemessung – unter Berücksichtigung der general- und spezialpräventiven Aspekte – erfolgte. Demgemäß fehlt im Akt auch eine rechtliche Erörterung, warum die Voraussetzungen eines abgekürzten Verfahrens im konkreten Fall als gegeben angesehen wurden.

Im Rahmen der Erhebungen durch die Kommission wurde festgestellt, dass im Anlassfall bei der Verhängung der Disziplinarstrafe durch die Dienstbehörde zwei formale Fehler passiert sind. Erstens fehlte in dem Verweis eine Rechtsmittelbelehrung über die Möglichkeit eines Einspruchs gegen die Disziplinarverfügung gem. § 132 BDG 1979. Zweitens wurde die Disziplinarverfügung dem Disziplinaranwalt, dem ebenfalls ein Einspruchsrecht zusteht, zunächst nicht zugestellt. Dies wurde erst am 13. August 2025 nachgeholt. Die Ursache für dieses Versäumnis konnte nicht abschließend geklärt werden, jedoch deuten Aussagen von Auskunftspersonen auf eine tatsächliche Unkenntnis der Verfahrensvorschriften hin. Dies ist auf unterschiedliche Gründe zurückzuführen: Ein aus Sicht der Kommission überinterpretiertes Vertraulichkeitsverständnis („Need-to-know“-Prinzip) führte dazu, dass in Disziplinarangelegenheiten kaum ein über die Abteilung VI.1 hinausgehender fachlicher Austausch stattfindet. Ein solcher wäre einerseits mit dem Disziplinaranwalt möglich. Andererseits könnten rechtliche Fragen etwa mit Vertreter:innen der Bundesdisziplinarbehörde besprochen werden, ohne in Details des konkreten Falls zu gehen. Darüber hinaus wurde festgestellt, dass nicht allen in Disziplinarangelegenheiten zuständigen

Personen die einschlägigen Schulungs- und Fortbildungsmöglichkeiten der Verwaltungsakademie des Bundes bekannt sind und dementsprechend bisher auch nicht wahrgenommen wurden.

Im Bereich des Disziplinarrechts fehlt es außerdem an einem institutionalisierten ressortübergreifenden, die Bundesdisziplinarbehörde einbeziehenden Austausch der für Disziplinarangelegenheiten zuständigen Personen, der gerade für kleine Ressorts mit vergleichsweise geringer Praxiserfahrung zweckdienlich wäre.

Schließlich ist festzuhalten, dass eine vollständige, routinemäßige Überprüfung der Aussagen, die der betroffene Beamte im Disziplinarverfahren getätigt hatte, unterblieben ist. Dies betrifft beispielsweise dessen Aussage, wonach er lediglich den Blog betrieben habe, es aber nicht zu Handlungen gegenüber natürlichen Personen gekommen sei. Im Rahmen der von der Abteilung VI.7 durchgeführten technischen Analyse konnte laut der Aktenlage lediglich festgestellt werden, dass es einmalig zu einem Zugriffsversuch von einem, nicht näher bestimmten Dienstgerät kam, der jedoch softwareseitig vom BMEIA blockiert wurde. Hinsichtlich der Frage, ob dienstliche IKT-Geräte für den Betrieb des Blogs genutzt wurden oder ob der Blog vom Arbeitsplatz aus und/oder während der Dienstzeit betrieben wurde, stützte sich die Dienstbehörde ansonsten im Wesentlichen auf die verneinende Aussage des Beamten. Dazu ist anzumerken, dass die Bestimmungen des Unterabschnitts „IKT-Nutzung und Kontrollmaßnahmen“ (§§ 79c ff. BDG) aus Sicht der Kommission durchaus einen rechtlichen Rahmen für eine umfassende Nachschau geboten hätten. Mit den der Kommission zu Verfügung stehenden Mitteln (*Anmerkung:* keine Möglichkeit zur erweiterten Wayback-/Archive-Analyse) konnten zu diesen, auch in der Medienberichterstattung thematisierten Vorwürfen, keine Feststellungen getroffen werden.

iii. Zum Prozess betreffend die Entscheidung über eine Ab- und Einberufung:

Die (rechtlich jederzeit – auch ohne Angabe von Gründen – mögliche) Ab- und Einberufung von an österreichischen Vertretungsbehörden im Ausland tätigen Bediensteten als dienstrechtliche Maßnahme wird im BMEIA regelmäßig eingesetzt, sowohl bei Beamt:innen (u.U. kumulativ zu einem Disziplinarverfahren) also auch bei Vertragsbediensteten. Die untersuchte Praxis des BMEIA über den Anlassfall hinaus hat gezeigt, dass eine disziplinäre Maßnahme nicht zwingend eine Ab- und Einberufung zur Folge haben muss.

Auffallend ist, dass es für diese Maßnahme bis dato weder einen festgelegten und nachvollziehbaren Standardprozess gibt, noch einen einzuhaltenden Aktenlauf noch objektive und sachliche Kriterien zur Beurteilung der Frage, ob eine Ab- und Einberufung in einem konkreten Fall angemessen und vorzunehmen ist.

Als problematisch hervorzuheben ist, dass mangels eines Standardprozesses im Anlassfall keine Einbindung der Abteilung für Sicherheitsangelegenheiten erfolgte. Deren Einschätzung konnte daher nicht in den Entscheidungsprozess einfließen.

Unklar geblieben ist für die Kommission, wer letztendlich die Entscheidung getroffen hat, dass der betroffene Beamte in seiner Position verbleiben, d.h. nicht ab- und einberufen werden soll. Hierzu fehlt es an jeglichen Aufzeichnungen. Eine eindeutige Empfehlung der Sektion VI („Management“) gegenüber den weisungsbefugten Stellen, wie sie etwa im Bereich des Disziplinarwesens betreffend eine Disziplinarstrafe sehr wohl vorlag, wurde nicht dokumentiert. Fest steht, dass die Frage der Ab- und Einberufung in den bereits erwähnten Besprechungen zwischen dem Generalsekretär und Mitgliedern des Kabinetts des damaligen Bundesministers mit der Sektion VI diskutiert wurde. Der damalige Bundesminister war nach übereinstimmenden Aussagen von Auskunftspersonen über den Vorgang informiert.

Aus Sicht der Kommission lag der Entscheidung, den betroffenen Beamten im Anlassfall auf seiner Position zu belassen, eine Fehleinschätzung hinsichtlich des Risikos einer „externen Erpressbarkeit“, des öffentlichen Bekanntwerdens der festgestellten Tätigkeiten (insbesondere des von ihm betriebenen pornografischen Blogs) und damit eines Vertrauensverlusts der Allgemeinheit in die sachliche Wahrnehmung seiner dienstlichen Aufgaben (Reputationsschaden) zugrunde. Dies lässt sich u.a. auf - mangels Standardprozesse – fehlende Informationen und ungenügende Risikobewertungen zurückführen. Der Dienststellenausschuss hatte das Risiko eines öffentlichen Bekanntwerdens des Anlassfalls thematisiert und einstimmig für eine Ab- und Einberufung des betroffenen Beamten plädiert, doch fand dies im Entscheidungsprozess der weisungsbefugten Stellen keine Berücksichtigung.

Aus den Gesprächen ergab sich, dass die weisungsbefugten Stellen offensichtlich davon ausgingen, die Sache sei mit dem Disziplinarverfahren erledigt, obwohl ein weiteres Vorgehen der hinweisgebenden Person und ein öffentliches Bekanntwerden nicht ausgeschlossen werden konnte. Dies führte zu einem Reputationsschaden für das BMEIA sowie für die Republik Österreich.

iv. Feststellungen zum fehlenden Disziplinarrecht der Vertragsbediensteten

Der Anlassfall verdeutlicht auch die unterschiedliche Behandlung von Beamtinnen und Beamten einerseits und Vertragsbediensteten andererseits. Während der Beamte mit dienst- und disziplinarrechtlichen Folgen sanktioniert wurde, hätte ein gleich gelagerter Fall eines Vertragsbediensteten oder einer Vertragsbediensteten vermutlich keine arbeitsrechtlichen Konsequenzen nach sich gezogen, obwohl der potenzielle Reputationsschaden gleich gewesen wäre. Zu hoffen bleibt deshalb, dass die im aktuellen Regierungsprogramm vorgesehene „Prüfung der Annäherung der Verfahren bei Dienstpflichtverletzungen” zukünftig zu einem Ergebnis führt, das Gleiches gleichbehandelt.

c. Empfehlungen

Im Fall des Bekanntwerdens von Sachverhalten, die disziplinar- oder dienstrechtlich relevant sein könnten, erscheint es dringend geboten, klare Standardprozesse für die weitere Bearbeitung solcher Fälle im BMEIA festzulegen. Dies gilt auch für Meldungen an das Generalinspektorat gemäß dem HSchG oder in dessen Funktion als Ombudsstelle im BMEIA.

Dabei erscheint es im Lichte der Diversität und Komplexität der möglichen Sachverhalte sinnvoll, systematisch eine Erst- und eine Abschlussbewertung (einschließlich Risikobewertung) durch eine interdisziplinär zusammengesetzte Personengruppe vornehmen zu lassen. Dieser sollten jedenfalls Vertreterinnen und Vertreter der Abteilung für Personalangelegenheiten VI.1, Sicherheitsangelegenheiten I.2 und der Rechtsberater im BMEIA (Gruppenleiter I.A) angehören. Je nach Bedarf des Einzelfalls sollten im Rahmen des „Need-to-know"-Prinzips weitere Personen fachspezifisch hinzugezogen werden, beispielsweise aus den Bereichen IKT, Generalinspektorat oder Arbeitspsychologie. Darüber hinaus sollte diese Gruppe Empfehlungen für allfällige dienstrechtliche Maßnahmen, insbesondere für eine Abberufung vom Arbeitsplatz und Einberufung in die Zentrale, machen.

Bei Disziplinarverfahren zu Vorfällen, von denen andere Bedienstete betroffen sein könnten, sind Nachfragen bzw. Nachschauen bei diesen potentiell Betroffenen in einem geeigneten Rahmen zweckmäßig.

Es wäre sinnvoll, alle Prozessbeteiligten in disziplinar- und dienstrechtlichen Angelegenheiten frühzeitig über die Verpflichtung zur Meldung allfälliger Befangenheiten gemäß § 7 Allgemeinen Verwaltungsverfahrensgesetz 1991 hinzuweisen. In Fällen, die hochrangige Vertreterinnen und Vertreter des BMEIA betreffen, sollte die Möglichkeit geprüft werden, im Wege der Amtshilfe (Art. 22 Bundes-Verfassungsgesetz) externe Stellen für Erhebungszwecke beizuziehen. Diese beiden Aspekte sollten jedenfalls Teil der eingangs angeführten Standardprozesse sein.

Mit dem Inkrafttreten des HSchG wurde das Generalinspektorat als „Kontaktstelle der Bundesdisziplinarbehörde für Meldungen nach dem HSchG im Bereich des BMEIA" festgelegt. Im Hinblick auf dessen Tätigwerden in dieser Funktion stellt sich die Frage der Anwendbarkeit der „Revisionsordnung für das Bundesministerium für europäische und internationale Angelegenheiten", die gegebenenfalls eine Berichtspflicht auslösen könnte. Dieser Aspekt bedarf einer Klarstellung (u.a. im Lichte der Vorgaben des HSchG). Generell wäre die Revisionsordnung und die Rahmenbedingungen für das Tätigwerden des Generalinspektorats im Sinne internationaler Standards regelmäßig zu evaluieren, zu aktualisieren und an „Best practice"-Modelle anzupassen.

Um eine konsistente Behandlung aller Disziplinarfälle im Sinne des Gleichbehandlungsgebotes sicherzustellen, empfiehlt die Kommission, im Lichte der bisherigen Disziplinarverfahrenspraxis des BMEIA sowie der Rechtsprechung der Bundesdisziplinarbehörde nachvollziehbare Kriterien festzulegen. Diese sollten zur Beurteilung herangezogen werden, ob eine Dienstpflichtverletzung vorliegt, angesichts derer eine Belehrung bzw. Ermahnung nicht mehr ausreicht, welches Verfahren zu wählen ist (abgekürztes Verfahren gemäß § 131f BDG 1979 oder Weiterleitung der Disziplinaranzeige an die Bundesdisziplinarbehörde gemäß § 110 Abs. 1 Z 2 BDG 1979), und welche Disziplinarstrafe im Falle eines abgekürzten Verfahrens zu erfolgen hat.

Zur Stärkung der Nachvollziehbarkeit von Entscheidungen in Disziplinarverfahren hält die Kommission eine grundsätzliche, aktenmäßige Befassung des Generalsekretärs als des obersten Beamten des Ressorts für angebracht. Zudem sollten Kriterien festgelegt werden, die je nach Sachverhalt und betroffener Person eine Befassung der Ressortleitung im Aktenwege vorsehen.

Ebenso bedarf es aus Sicht der Kommission einer Verbesserung der Aktenführung in Disziplinarverfahren. Sämtliche Erhebungsschritte müssen belegt und die Erkenntnisse bzw. Bewertungen festgehalten werden.

Die Rechtsprechung der Bundesdisziplinarbehörde bzw. des Bundesverwaltungsgerichts könnte durch eine, z.B. jährlich erscheinende, Zusammenfassung wesentlicher Entscheidungen zugänglicher gemacht werden.

Um ressortübergreifend eine stärkere Gleichbehandlung von Disziplinarfällen zu erreichen und den Wissens- und Erfahrungsaustausch vor allem für kleinere Ressorts zu stärken, könnte eine jährliche gemeinsame Tagung für die Disziplinarrechtsreferentinnen und -referenten aller Bundesministerien angeregt werden. Eine solche Veranstaltung würde auch den informellen und - bezogen auf konkrete Fälle - anonymisierten Austausch der Disziplinarrechtsreferentinnen und -referenten untereinander und mit der Bundesdisziplinarbehörde fördern; eine Möglichkeit, die aus Sicht der Kommission die Entscheidung von Disziplinarfälle auf einfachem Wege erleichtern könnte.

Informations- und Fortbildungsmöglichkeiten im Bereich Dienst- und Disziplinarrecht (z.B. im Rahmen der Verwaltungsakademie des Bundes) sollten den im BMEIA für diesen Themenbereich zuständigen Personen nahegelegt und in sinnvollen Abständen von diesen verpflichtend wahrgenommen werden.

Da im BMEIA auch die disziplinar- und dienstrechtlich relevanten Bereiche zu einem Großteil dem Rotationsprinzip im Zuge von Personalbesetzungen unterliegen, ist eine Verbesserung des Wissensmanagements unumgänglich. Abgesehen von dem bereits erwähnten Festlegen von Standardprozessen und Kriterien, sollten vermehrt Vorlagen für ELAK-Prozessläufe, Checklisten (z.B. für die Aktenführung) und (Format-)Vorlagen (z.B. für Disziplinarverfügungen) erstellt werden und zum Einsatz gelangen.

Die Erhebungen durch die Kommission haben gezeigt, dass in einzelnen Tätigkeitsbereichen des BMEIA, denen eine spezielle Expertise und Erfahrung erfordernder Aufgabenbereich zukommt, eine verstärkte Professionalisierung angestrebt und entsprechende Maßnahmen der Personalentwicklung getroffen werden sollten. Beispielsweise sollten gewisse einschlägige Aus- und Fortbildungen ermöglicht und bei der Ausschreibung dieser Stellen zur Bewerbungsvoraussetzung gemacht werden.

Die Kommission ist der Ansicht, dass der Anlassfall umfassender behandelt worden wäre, wenn die Abteilung I.2 (Sicherheitsangelegenheiten) frühzeitig eingebunden worden wäre. Es sollte geprüft werden, wie deren Auftrag - personelle, materielle und IKT-Sicherheit in der Zentrale und rund 100 Standorten im Ausland - bestmöglich gewährleistet werden kann. Dazu gehört nicht nur eine Prüfung des Personalstands sowie der Schaffung einer eigenen Budgetlinie, sondern etwa auch der Vorschlag der Bestellung regionaler Sicherheitsverantwortlicher für besonders exponierte Standorte, beispielsweise in Brüssel, in gewissen Staaten am afrikanischen Kontinent sowie im Nahen bzw. Mittleren Osten. Deren Aufgabenbereich sollte jährliche Schulungen (einschließlich „Computerbased Schulungen“) samt Wissensüberprüfung der entsandten und lokalen Mitarbeiterinnen und Mitarbeiter in Sicherheitsfragen umfassen (einschließlich der besonderen Gefährdung durch Erpressbarkeit für die Bediensteten, ihre

Familien und die Republik Österreich insgesamt). Darüber hinaus sollte das Mandat die Beobachtung der lokalen bzw. regionalen Sicherheitssituation, die Beratung der Vertretungsbehörden vor Ort und die Durchführung von Krisenübungen einschließen.

Die Kommission kann mangels eigener Befugnis zu Ermittlungen angesichts der im Hinweis vorgebrachten Sachverhalte einen Anfangsverdacht im Sinne des Strafgesetzbuches nicht abschließend und ausschließend prüfen. Sie empfiehlt daher, diesen Sachverhaltskomplex der Staatsanwaltschaft zur allfälligen weiteren Abklärung zu übergeben.

2. Sicherheit der IKT-Systeme des BMEIA

Dieser Berichtsteil basiert auf Erfahrungen bei der Behandlung von mehreren Vorfällen, u.a. jenen des Government Computer Emergency Response Teams (GovCERT) im Bereich des öffentlichen Dienstes, auf Interviews der Kommission, die im August und September 2025 mit Mitarbeiterinnen und Mitarbeitern des BMEIA geführt wurden, sowie diversen Dokumenten, die der Kommission zur Verfügung gestellt wurden. Um die Integrität der IKT-Infrastruktur des BMEIA vor Angriffen aus dem In- und Ausland zu schützen, werden im Folgenden Erkenntnisse der Kommission teilweise nur kursorisch skizziert.

a. Ergebnis der Erhebungen

Das BMEIA ist in Bezug auf Cyberangriffe in einer exponierten Position in Österreich. Die ab 2009 beobachteten Angriffe waren gezielt gegen das BMEIA gerichtet, die Tätergruppen sind bekannten staatlichen Akteuren zuordenbar. Das steht im Gegensatz zu den meisten anderen Fällen in der öffentlichen Verwaltung, bei denen es sich um „targets of opportunity“ gehandelt hat, wo die Tätergruppen ungezielt verwundbare Systeme angegriffen haben.

Im BMEIA wurde dieser Tatsache 2010 Rechnung getragen, indem erste „Grundsätze der Informationssicherheit im BMeiA“ festgelegt wurden. Darin wurden auf sehr hohem Niveau die Schutzziele, generelle Richtlinien und die Zuständigkeiten festgelegt:

Die Abteilung I.2 (Sicherheit) soll:

- Die Rolle des Informationssicherheitsbeauftragen (nach innen und in Richtung Informationssicherheitskommission) einnehmen,
- IKT-Sicherheitskonzepte entwickeln,
- Sicherheitsbewertungen von Beschaffungen und Eigenentwicklungen durchführen,
- organisatorische Maßnahmen bzgl. IKT-Sicherheit einleiten,
- Schulungen durchführen,
- Strategien zur Erkennung von Risiken entwickeln und
- die Wirksamkeit der Maßnahmen in Form von Audits regelmäßig bewerten

Die Abteilung VI.7 (IKT) soll:

- Technische Aspekte und Maßnahmen der IKT-Sicherheit laut Vorgaben und Konzepten umsetzen und betreuen,
- bei der Entwicklung der Konzepte mitarbeiten,
- operativ bei Sicherheitsvorfällen agieren und
- die Dokumentation der IKT-Sicherheit aktuell halten.

Zur Koordination wurde das Gremium „Informationssicherheitsmanagement-Team“ (ISM-T) eingerichtet, das auch Richtlinien und Sicherheitskonzepte festlegen kann und deren Umsetzung kontrollieren soll. Das ISM-T setzt sich aus Vertreterinnen und Vertretern des Generalsekretärs, der Abteilung I.2, der Abteilung VI.7 und des Generalinspektorats zusammen.

b. Bewertung durch die Untersuchungskommission

Der „Lessons Learned“-Prozess nach den IKT-Sicherheitsvorfällen zwischen 2009 und 2020 wurde nicht systematisch geführt. Zwar wurden auf der Seite der direkt mit Sicherheitsagenden betrauten Technikerinnen und Technikern der Abteilung VI.7 relevante und mit Blick auf spätere Cyberangriffe hilfreiche Maßnahmen umgesetzt, die Involvierung anderer Teams der Abteilung war jedoch nicht klar erkennbar.

Der Eindruck der Kommission ist, dass einzelne Mitarbeiterinnen und Mitarbeiter über die Jahre hinweg mit hoher Eigenmotivation und Fachwissen gute Arbeit geleistet haben. Sie bekamen jedoch in der Hierarchie des BMEIA nicht die Unterstützung, Ressourcen und Führung, die nötig gewesen wären, um aus Einzelleistungen ein konsistentes, von allen Stellen mitgetragenes und laufend kontrolliertes sowie verbessertes Sicherheitsnetz zu bilden.

Die Erkenntnisse der Kommission zeigen dennoch, dass das BMEIA aus den Cybervorfällen der Vergangenheit gelernt hat und auf einem grundsätzlich richtigen Weg ist. Einige sehr fähige Mitarbeiterinnen und Mitarbeiter in der Informationssicherheit (Abt. I.2) und ITSicherheit (Abt. VI.7), die bereits heute tragende Rollen übernehmen, sind hier besonders hervorzuheben. Zudem wurde 2024 ein Projekt zur Etablierung eines Informationssicherheitsmanagementsystems (ISMS) gestartet – ein wichtiger Schritt, um die Sicherheit im BMEIA systematisch zu verankern und die Steuerungsfähigkeit nachhaltig zu stärken. Diese positive Ausgangslage bildet eine gute Basis, um die identifizierten Risiken zügig und wirksam zu adressieren.

Gleichzeitig wurde deutlich, dass die organisatorische Einordnung der Informationssicherheit verbessert werden muss. Derzeit fehlt eine klar mandatierte Gesamtverantwortung mit eindeutigen Befugnissen und Berichtswegen. Das führt zu Verzögerungen in Entscheidungen, zu Überschneidungen in Aufgaben und zu einer uneinheitlichen Priorisierung. Für ein Ministerium mit internationaler Präsenz ist dies kritisch, weil es die Wahrscheinlichkeit und den möglichen Umfang von Sicherheitsvorfällen erhöht. Eine klare Platzierung der Informationssicherheit im System des BMEIA fehlt: Es gibt keinen „Chief

Information Security Officer“ (CISO) als Stabsstelle und keine direkte, regelmäßige Berichtspflicht an den Generalsekretär. Infolge der unklaren Verantwortlichkeiten mangelt es bereichsübergreifend an Transparenz, Entscheidungsfähigkeit und Durchsetzungskraft; der Aufwand zur Klärung wäre gering, die Wirkung unmittelbar.

Die fehlende zentrale Nachverfolgung und Wirksamkeitsmessung von Sicherheitsmaßnahmen sind eng mit der Verantwortungsfrage verbunden. Aktuell sind Empfehlungen und Maßnahmen in verschiedenen, zum Teil nicht verknüpften Dokumenten und Berichten zu finden. Dadurch fehlt der konsolidierte Überblick: Prioritäten, Fristen, Zuständigkeiten und messbare Zielgrößen werden nicht einheitlich gesteuert, und die BMEIA-Führung erhält keine verlässlichen Gesamtkennzahlen zum Fortschritt. Die Folge sind offene Maßnahmen, deren Wirkung nicht überprüft ist, sowie eine eingeschränkte Steuerungsfähigkeit, was nicht im Sinne eines kontinuierlichen Verbesserungsprozesses ist. Auch dies ließe sich rasch und mit geringem Aufwand verbessern, indem alle offenen Sicherheitsmaßnahmen und Risiken zentral geführt, nachverfolgt und regelmäßig berichtet werden. Ein solches konsolidiertes Reporting stärkt die Managementbewertung unmittelbar, macht Fortschritte sichtbar und ermöglicht rechtzeitige Eskalationen, wo es nötig ist.

Darüber hinaus besteht Handlungsbedarf in der Koordination von Audits und Prüfungen. Aktuell werden unterschiedliche technische und prozessuale Prüfungen in verschiedenen Bereichen beauftragt, teils ohne wechselseitige Kenntnis. Das birgt das Risiko von Doppelarbeit, Lücken und ineffizientem Budgeteinsatz. Vor allem verhindert es, dass Feststellungen systematisch in ein zentrales Risikomanagement überführt und deren Umsetzung verlässlich nachverfolgt wird. Ein abgestimmtes, mehrjähriges Auditprogramm unter Führung des ISMS würde sicherstellen, dass alle relevanten Themen abgedeckt sind, Wiederholungsprüfungen geplant werden und Ergebnisse einheitlich in Maßnahmen und Risikosteuerung einfließen. Die Arbeitsteilung genauso wie eine enge Abstimmung zwischen den Abteilungen I.2 und VI.7 sind hier entscheidend; die organisatorische Klarstellung und das zentrale MaßnahmenTracking liefern dafür die notwendige Grundlage.

Ergänzend zeigt die Untersuchung, dass eine flächendeckende, wirksame AwarenessStrategie fehlt. Die bisherige Schulungsreichweite ist angesichts der globalen Verteilung und Mitarbeitendenzahl nicht ausreichend, und ein verbindlicher, messbarer Programmansatz ist nicht erkennbar. Das erhöht die Erfolgsquote typischer Angriffe wie Phishing und Social Engineering und führt dazu, dass Vorfälle später erkannt und gemeldet werden.

Dabei ist anzumerken, dass Logdaten und die forensische Untersuchung von Geräten durchaus sensible Daten über Mitarbeitende enthalten können. Aus diesem Grund wird üblicherweise zwischen Auswertungen aus sicherheitsrelevanten Themen und Auswertungen nach dienst- bzw. disziplinarrechtlichen Kriterien unterschieden. In manchen anderen Organisationen ist auch explizit geregelt, ob und unter welchen Bedingungen Daten, die aus sicherheitsrelevanten Gründen erhoben wurden, für andere Zwecke verwendet werden dürfen.

Anlässlich der Vorfallsbehandlung 2019/2020 wurde in erster Linie der Fokus auf die sicherheitsrelevanten Aspekte gelegt, um unter anderem die schnellstmögliche Wiederherstellung des Dienstbetriebs zu ermöglichen. Die Namen der betroffenen Accounts wurden in diesem Zusammenhang lediglich als technisches Detail behandelt. Bewertungen, ob eine Verletzung von Dienstpflichten (z.B. grob fahrlässiges Fehlverhalten einzelner Bediensteter) vorliegen könnte, wurden bewusst nicht getroffen. In der IT-Sicherheit wird davon ausgegangen, dass bei einer großen Zahl von Nutzerinnen und Nutzern Fehler gemacht werden. Wer konkret der Einfallsvektor war, ist für die Behandlung des Vorfalls nicht relevant.

Wie bei den meisten dieser Vorfälle, so war auch der Erfolg des Angriffs von 2019/2020 erst durch eine Reihe von Fehlern in der Verteidigung in der beobachteten Form möglich. Es wurden von mehreren Seiten kritische Fehler gemacht, ein kompromittiertes Passwort eines von insgesamt ca. 2400 Nutzerinnen und Nutzern wurde damals als wenig überraschend eingeschätzt. Der Frage, wie dieses Passwort verloren wurde, ist man nicht nachgegangen. Heute, fast sechs Jahre später, lässt sich diese Frage nicht mehr beantworten und damit auch nicht, ob eine grob fahrlässige Handlung des betroffenen Beamten vorlag. Dass es irgendeinen Zusammenhang zu dem Betrieb des Blogs durch den betroffenen Beamten oder andere private Aktivitäten seinerseits gibt, ist aus Sicht der Kommission reine Spekulation.

Hinsichtlich der medial kolportierten Verbindung zwischen dem IKT-Fehlverhalten des leitenden Beamten und dem Cyberangriff auf die Infrastruktur der BMEIA im Jahr 2019 konnte die Kommission keinen unmittelbaren Kausalzusammenhang belegen. Festgestellt wurde jedoch, dass der Rechner des betroffenen Beamten eines der kompromittierten Systeme war.

c. Empfehlungen

Aus Sicht der Kommission wäre es empfehlenswert, zunächst die beiden schnell und ressourcenschonend realisierbaren Schritte anzugehen: die eindeutige Mandatierung der Informationssicherheit mit direkter Berichtspflicht an den Generalsekretär sowie den Aufbau eines zentralen, kennzahlenbasierten Maßnahmen und RisikoReportings. Beides stärkt innerhalb weniger Wochen die Steuerungsfähigkeit und legt das Fundament für alle weiteren Vorhaben. Darauf aufbauend sind die strukturellen Maßnahmen mit höherer Reichweite, aber längerem Vorlauf, entschieden voranzutreiben: die Netzsegmentierung in den Auslandsvertretungen mit klarer Terminierung und Fortschrittskontrolle, die Etablierung eines abgestimmten, mehrjährigen Auditprogramms und der Rollout eines verbindlichen „AwarenessProgramms“ mit ressortweiter Reichweite (Zentrale und Vertretungsbehörden). Diese Themen greifen ineinander: Ein zentrales Reporting macht Fortschritte und Risiken sichtbar, die Auditkoordination liefert belastbare Erkenntnisse für Prioritäten, und Awareness unterstützt die Wirksamkeit technischer und organisatorischer Schutzmaßnahmen.

Um ein höheres, resilienteres IKT-Sicherheitsniveau im BMEIA zu verankern, empfiehlt die Kommission die Erarbeitung eines Aus- und Fortbildungsprogramms. Dieses sollte alle Zielgruppen regelmäßig erreichen, den Lernerfolg nachverfolgen und Fortschritte messbar machen. Das Thema eines sicheren Umgangs mit IKT Systemen inklusive Bewusstseinsbildung für Angriffe aller Art (technische Angriffe, „social engineering“, „information operations“) ist etwa für alle Mitarbeiterinnen und Mitarbeiter des BMEIA

äußerst relevant. In den Abteilungen I.2 und VI.7 sind Aus- und Fortbildungsmaßnahmen zu Fachthemen (z.B. sichere Softwareentwicklung, Sicherheitskonzepte in Windows-Netzwerken, Informationssicherheitsmanagement, etc.) zweckdienlich. Dies ist zwar kein Sofortthema wie die organisatorischen „Quick Wins“, sollte aber zeitnah begonnen werden, um in einem angemessenen Zeitraum spürbare Wirkung zu entfalten.

Als klaren Zielpunkt empfehlen wir die Zertifizierung des ISMS nach ISO/IEC 27001 mit Meilenstein Anfang des Jahres 2027. Die Zertifizierung schafft Verbindlichkeit, definiert einen überprüfbaren Meilenstein und verankert den kontinuierlichen Verbesserungsprozess („Plan-Do-Check-Act“) institutionell. Damit verpflichten sich sowohl ISMS-Organisation als auch Führung, das Sicherheitsniveau messbar zu steigern und die Fortschritte regelmäßig extern überprüfen zu lassen.

Darüber hinaus empfiehlt die Kommission die Einrichtung einer ressortübergreifenden zentralen Sicherheitsorganisation, die für alle Ministerien verbindliche und konkrete Mindestanforderungen, Standards und Berichtspflichten festlegt und deren Einhaltung regelmäßig prüft. Eine solche Instanz stellt ein einheitliches Sicherheitsniveau sicher, erhöht Transparenz und Vergleichbarkeit und ermöglicht schnelleres Lernen aus Vorfällen und Prüfungen. Zugleich bündelt sie Expertise und Ressourcen, reduziert Doppelaufwände und stärkt die Krisenreaktionsfähigkeit über Ressortgrenzen hinweg. Die Umsetzung der EU-Richtlinie NIS-2 in Österreich bietet sich als Hebel dafür an. Die dort definierten Sicherheitsstandards für wichtige und wesentliche Einrichtungen werden in Zukunft auch für die öffentliche Verwaltung verpflichtend sein.

Die Untersuchung bestätigt damit sowohl die vorhandenen Stärken als auch die wesentlichen Hebel für schnelle und nachhaltige Verbesserungen. Mit den motivierten Mitarbeiterinnen und Mitarbeiter in den Abteilungen I.2 und VI.7 und dem geplanten ISMSStart noch im Jahr 2025 sind die Voraussetzungen gegeben, das Sicherheitsniveau zügig und messbar zu erhöhen. Entscheidend ist nun, die Informationssicherheit organisatorisch passend zu positionieren, klare Verantwortlichkeiten und Berichtswege zu definieren und schriftlich zu fixieren, sowie die Transparenz über Maßnahmen und Risiken herzustellen. In einem nächsten Schritt müssen die konkret ausgearbeiteten Maßnahmenempfehlungen folgen, die der BMEIA-Führung zur Entscheidung vorzulegen sein werden.

3. Möglichkeit der Einflussnahme auf den betroffenen Beamten

a. Ergebnis der Erhebungen

Der Anlassfall für die Untersuchung hat auch die Frage aufgeworfen, ob der betroffene Beamte aufgrund einer latenten Erpressbarkeit Ziel einer Einflussnahme durch externe Akteure (z.B. ausländische Nachrichtendienste) gewesen sein könnte. Auch wenn die abschließende Klärung dieser Frage in erster Linie in die Zuständigkeit der Sicherheitsbehörden fällt, liegen der Kommission nach dem derzeitigen Kenntnisstand keine entsprechenden Indikationen vor.

Hinsichtlich des medial dargestellten sicherheitsrelevanten Aspekts, Dritte hätten sich offenbar Zugang zu dienstlichen Geräten des betroffenen Beamten verschafft und so auch Zugriff auf dienstliche Informationen erlangt, legen die Erhebungen der Kommission mit den ihr zu Verfügung stehenden Mitteln nahe, dass es nur zu Zugriffen auf zu diesem Zeitpunkt unversperrte dienstliche Geräte des betroffenen Beamten durch eine Person in seinem privaten Umfeld kam.

Nach den Erhebungen der Kommission mit den ihr zu Verfügung stehenden Mitteln liegen keine Indizien vor, die die Behauptungen in der Medienberichterstattung, Bildaufnahmen des pornografischen Blogs wären bereits seit längerer Zeit im Arbeitsumfeld des betroffenen Beamten zirkuliert und er sei möglicherweise von Mitarbeiterinnen oder Mitarbeitern erpresst worden, die sich etwa damit Posten erzwungen hätten, stützen würden.

b. Bewertung durch die Untersuchungskommission und Empfehlungen

Aus Sicht der Kommission sollten Standardprozesse für den Fall des Aufkommens von Verdachtsmomenten der externen Einflussnahme auf BMEIA-Bedienstete festgelegt werden. So sollte beispielsweise die rasche Abnahme von und die weitere Behandlung dienstlicher Geräte klar geregelt werden.

Losgelöst vom konkreten Fall ist festzuhalten, dass Angehörige des auswärtigen Dienstes in hohem Maße der Gefahr externer Einflussnahme bzw. Beeinflussung ausgesetzt sind. Aus diesem Grund erscheint es angezeigt, bereits ab der Personalrekrutierung und insbesondere bei der Betrauung mit Leitungsfunktionen darauf zu achten, integre und möglichst untadelige Persönlichkeiten auszuwählen. Es wird empfohlen, Sicherheitsüberprüfungen nicht nur in periodischen Abständen, sondern auch aus Anlass der Versetzung auf besonders hochrangige bzw. exponierte Positionen im In- und Ausland vornehmen zu lassen. Dabei sollte überlegt werden, ob eine periodische erweiterte Sicherheitsüberprüfung bei gewissen Auslandsverwendungen angezeigt erschiene. Im Allgemeinen sollte geprüft werden, ob das Online-Verhalten von Personen (z.B. Postings auf Social Media) im Rahmen von Sicherheitsüberprüfungen in gewissem Ausmaß berücksichtigt werden dürfte.

In diesem Sinne empfiehlt es sich auch, bei Aus- und Fortbildungsmaßnahmen immer wieder auf den Aspekt der Erpressbarkeit und die damit einhergehende Gefährdung der persönlichen und/oder nationalen Sicherheit einzugehen. Solche Sensibilisierungs- und Präventionsmaßnahmen sowie „Debriefings“ nach Auslandsverwendungen könnten beispielsweise im Austausch mit anderen Behörden durchgeführt werden, die mit ähnlichen Bedrohungen konfrontiert sind.

Wien, 06. Oktober 2025

Der Vorsitzende:

(Thomas Starlinger)

	Unterzeichner	Parlamentsdirektion
	Datum/Zeit-UTC	2025-10-07T15:29:54+02:00
Prüfinformation	Dieses Dokument wurde elektronisch besiegelt. Informationen zur Prüfung des elektronischen Siegels und des Ausdrucks finden Sie unter: https://www.parlament.gv.at/siegel	