Bundesverwaltungsgericht
Tribunal administratif fédéral
Tribunale amministrativo federale
Tribunal administrativ federal

Abteilung I
A-700/2015

Urteil vom 26. Mai 2015

Besetzung

Richter Jürg Steiger (Vorsitz),
Richter Maurizio Greppi,
Richterin Kathrin Dietrich,
Gerichtsschreiber Matthias Stoffel.

Parteien

A._____,

gegen

Dienst Überwachung Post- und Fernmeldeverkehr (ÜPF),
Fellerstrasse 15, 3003 Bern,
Vorinstanz.

Gegenstand

Zugang zu amtlichen Dokumenten gemäss BGÖ.

Sachverhalt:

A.
Mit E-Mail vom 20. Juni 2013 ersuchte A._____ (Gesuchsteller) den Dienst für die Überwachung des Post- und Fernmeldeverkehrs (Dienst ÜPF) um Zugang zu einer "Liste der Namen und Versionsnummern aller Softwareprodukte […], welcher der Dienst ÜPF […] zur Erledigung aller seiner Tätigkeiten benötigt". Er bat weiter darum, in der Liste erkenntlich zu machen, welche der aufgeführten Softwareprodukte Eigenentwicklungen sind beziehungsweise welche im Auftrag des Dienstes ÜPF erstellt wurden und zu welchen Letzterer Zugriff auf den Quellcode hat.

B.
Der Dienst ÜPF bestätigte dem Gesuchsteller mit E-Mail vom 24. Juni 2013, dass ein oder mehrere Inventare der verwendeten Softwareprodukte bestünden, wies das Einsichtsgesuch jedoch ab. Aufgrund des Datenschutzes, des Schutzes des Fernmeldegeheimnisses sowie der Gefahr allfälliger Angriffe auf das System des Dienstes sei die Bekanntgabe der verwendeten Software unter allen Umständen zu vermeiden. Insbesondere stünden damit auch die zielkonforme Durchführung konkreter behördlicher Massnahmen, die Beziehungen zwischen dem Bund und den Kantonen sowie die innere Sicherheit und letztlich das Ansehen der Schweiz auf dem Spiel.

C.
Mit Schreiben vom 27. Juni 2013 reichte der Gesuchsteller beim Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) einen Schlichtungsantrag ein. Der Dienst ÜPF liess sich dazu mit Stellungnahme vom 5. Juli 2013 vernehmen und bekräftigte im Wesentlichen seine bisherige Argumentation, präzisierte jedoch, dass lediglich ein Verzeichnis der vom gesamten Informatik Service Center ISC-EJPD verwendeten Standardsoftware vorhanden sei. Eine diesbezüglich auf den Dienst ÜPF beschränkte Auflistung könne erstellt und offengelegt werden. Die Software zur Umsetzung der strafprozessualen Überwachung sei dagegen weder in kompletten Listen erfasst noch könne der Zugang dazu gewährt werden. Der EDÖB folgte diesem Standpunkt und erliess am 26. November 2014 die Empfehlung, dem Begehren lediglich bezüglich der Standardsoftware stattzugeben, im Übrigen jedoch abzuweisen.

D.
In der Folge gelangte der Gesuchsteller mit Eingabe vom 5. Dezember 2014 an den Dienst ÜPF und ersuchte um Erlass einer anfechtbaren Verfügung. Diese erging gestützt auf Art. 15 Abs. 1 des Öffentlichkeitsgesetzes vom 17. Dezember 2004 [BGÖ, SR 152.3] am 23. Dezember 2014 und hiess in Übereinstimmung mit der Empfehlung des EDÖB das Gesuch hinsichtlich einer Liste mit der eingesetzten Standardsoftware gut. Im Übrigen lautete der Entscheid unter Berufung auf die bereits genannten Gründe auf Abweisung.

E.
Gegen diese Verfügung erhebt der Gesuchsteller (Beschwerdeführer) am 2. Februar 2015 Beschwerde beim Bundesverwaltungsgericht. Er beantragt die Aufhebung der Verfügung sowie sinngemäss die Aushändigung von Listen mit den Namen und Versionsnummern aller Softwareprodukte, welche zur Ausleitung und Erfassung (Ziff. 1 a), Ausscheidung, Auswertung und Aufbereitung (Ziff. 1 b), Speicherung und Archivierung (Ziff. 1 c) sowie elektronischen Übermittlung (Ziff. 1 d) von Daten im Rahmen der Überwachungstätigkeit Anwendung finden. Ferner seien die zur Absicherung der technischen Infrastruktur (Ziff. 1 e) sowie die übrigen, nicht bereits bekanntgegebenen Softwareprodukte (Ziff. 1 f) in entsprechenden Auflistungen herauszugeben. Eventualiter sei die Verfügung aufzuheben und die Sache zur neuen Entscheidung an den Dienst ÜPF (Vorinstanz) zurückzuweisen (Ziff. 2). Zur Begründung bringt der Beschwerdeführer zusammenfassend vor, der Zugang zu den gewünschten Informationen würde die Überwachungsmassnahmen nicht beeinträchtigen und sei in Missachtung von Grundrechten verweigert worden.

F.
In ihrer Vernehmlassung vom 13. März 2015 schliesst die Vorinstanz auf Abweisung der Beschwerde.

G.
Der Beschwerdeführer hält seinerseits in seinen Bemerkungen vom 17. April 2015 vollumfänglich an der Beschwerde fest.

H.
Auf weitergehende Ausführungen und die sich bei den Akten befindlichen Schriftstücke wird, soweit entscheidwesentlich, in den nachfolgenden Erwägungen eingegangen.

Das Bundesverwaltungsgericht zieht in Erwägung:

1.

1.1 Gemäss Art. 31 VGG beurteilt das Bundesverwaltungsgericht Beschwerden gegen Verfügungen nach Art. 5 VwVG. Da keine Ausnahme nach Art. 32 VGG vorliegt und eine Vorinstanz nach Art. 33 Bst. d VGG verfügt hat, ist das Bundesverwaltungsgericht zur Beurteilung der vorliegenden Beschwerden gegen die Verfügung vom 23. Dezember 2014 zuständig (vgl. auch Art. 16 Abs. 1 BGÖ, der auf die allgemeinen Bestimmungen über die Bundesrechtspflege hinweist).

1.2 Zur Beschwerde ist berechtigt, wer vor der Vorinstanz am Verfahren teilgenommen oder keine Möglichkeit zur Teilnahme erhalten hat, durch die angefochtene Verfügung besonders berührt ist und ein schutzwürdiges Interesse an deren Aufhebung oder Änderung hat (Art. 48 Abs. 1 VwVG). Der Beschwerdeführer ist mit seinem Gesuch nicht vollumfänglich durchgedrungen, durch die angefochtene Verfügung auch materiell beschwert und demzufolge ohne Weiteres zur Beschwerde legitimiert.

1.3 Auf die frist- und formgerecht eingereichten Beschwerde (Art. 50 und 52 VwVG) ist daher einzutreten.

2.

Das Bundesverwaltungsgericht überprüft die angefochtene Verfügung auf Rechtsverletzungen – einschliesslich unrichtiger oder unvollständiger Feststellung des rechtserheblichen Sachverhalts und Rechtsfehler bei der Ausübung des Ermessens – sowie auf Angemessenheit hin (Art. 49 VwVG). Es wendet das Recht von Amtes wegen an und ist an die Begründung der Begehren der Parteien nicht gebunden (Art. 62 Abs. 4 VwVG).

3.

Das Öffentlichkeitsgesetz bezweckt, die Transparenz über den Auftrag, die Organisation und die Tätigkeit der Verwaltung zu fördern (Art. 1 BGÖ), damit Bürgerinnen und Bürger politische Abläufe erkennen und beurteilen können. Nebst Vertrauen soll dadurch das Verständnis für die Verwaltung und ihr Funktionieren gefördert sowie die Akzeptanz staatlichen Handelns erhöht werden (BGE 133 II 209 E. 2.3.1; BVGE 2011/52 E. 3; Urteil des BVGer A-1784/2014 vom 30. April 2015 E. 3.1). Zu diesem Zweck statuiert das BGÖ das Prinzip der Öffentlichkeit mit Geheimhaltungsvorbehalt und gewährt einen grundsätzlichen Anspruch auf Zugang zu amtlichen Dokumenten (Art. 6 Abs. 1 BGÖ; vgl. BGE 136 II 399 E. 2.1 mit Hinweisen;

PASCAL MAHON/OLIVIER GONIN, in: Brunner/Mader [Hrsg.], Öffentlichkeitsgesetz, Handkommentar, Bern 2008 [nachfolgend: Handkommentar BGÖ], Art. 6 Rz. 11 ff.).

3.1 Das BGÖ gilt für die gesamte Bundesverwaltung (Art. 2 Abs. 1 Bst. a BGÖ). Aus der Botschaft zum Bundesgesetz über das Öffentlichkeitsprinzip der Verwaltung vom 12. Februar 2003, BBl 2003 1963 (Botschaft zum BGÖ) folgt, dass der Begriff der Bundesverwaltung im BGÖ sowohl die zentrale Verwaltung samt den Departementen und der Bundeskanzlei als auch die dezentralen Verwaltungseinheiten umfasst (Botschaft zum BGÖ, S. 1985 f.; Urteil des BVGer A-590/2014 vom 16. Dezember 2014 E. 6.3).

Die Vorinstanz erfüllt ihre Aufgaben selbständig, ist weisungsungebunden und dem zuständigen Departement nur administrativ unterstellt (Art. 2 Abs. 2 des Bundesgesetzes vom 6. Oktober 2000 betreffend die Überwachung des Post- und Fernmeldeverkehrs [BÜPF]). Damit ist sie zur dezentralen Bundesverwaltung gemäss Art. 2 Abs. 3 des Regierungs- und Verwaltungsorganisationsgesetzes vom 21. März 1997 (RVOG, SR 172.010) in Verbindung mit Art. 7a Abs. 1 Bst. b der Regierungs- und Verwaltungsorganisationsverordnung vom 25. November 1998 (RVOV, SR 172.010.1) zu zählen, die dem Eidgenössischen Justiz- und Polizeidepartement (EJPD) administrativ zugeordnet ist (vgl. Anhang 1 RVOV). Als Teil der Bundesverwaltung fällt die Vorinstanz in den persönlichen Anwendungsbereich des BGÖ (Art. 2 Abs. 1 Bst. a BGÖ).

3.2 Zur Eingrenzung des sachlichen Geltungsbereichs führt Art. 3 Abs. 1 Bst. a Ziff. 1–6 BGÖ besondere Verfahrensarten auf, bei welchen das Öffentlichkeitsgesetz keine Anwendung findet. Gemäss Art. 3 Abs. 1 Bst. a Ziff. 2 BGÖ gilt das Gesetz nicht für den Zugang zu amtlichen Dokumenten betreffend Strafverfahren. Gemäss Botschaft zum BGÖ, S. 1989, wird der Zugang zu Dokumenten, die Teil der Verfahrensakten eines der in Art. 3 Abs. 1 Bst. a BGÖ aufgeführten Verfahren bilden, in den einschlägigen Spezialgesetzen geregelt. Dokumente, die zwar in einem weiteren Zusammenhang mit einem solchen Verfahren stehen, aber keinen Eingang in die Verfahrensakten im engeren Sinn finden, sind dagegen grundsätzlich nach dem Öffentlichkeitsgesetz zugänglich (Botschaft zum BGÖ, S. 2008). Eine solche einschränkende Auslegung der Ausnahmebestimmung von Art. 3 Abs. 1 Bst. a BGÖ entspricht auch dem mit dem BGÖ verfolgten Grundsatz der Öffentlichkeit mit Geheimhaltungsvorbehalt (vgl. SCHWEIZER/WIDMER, Handkommentar BGÖ, Art. 3 Rz. 12).

Bei den nachgesuchten Listen über die von der Vorinstanz im Rahmen ihrer Überwachungstätigkeit verwendeten Softwareprodukte handelt es sich um eine allgemeine Information über verwendete Arbeitsinstrumente im Strafverfahren, die als solche nicht Teil der Verfahrensakten ist. Das Einsichtsgesuch untersteht damit dem sachlichen Anwendungsbereich des BGÖ.

3.3 Als amtliches Dokument gilt gemäss Art. 5 Abs. 1 BGÖ jede Information, die auf einem beliebigen Informationsträger aufgezeichnet ist (Bst. a); sich im Besitz einer Behörde befindet, von der sie stammt oder der sie mitgeteilt worden ist (Bst. b); und die Erfüllung einer öffentlichen Aufgabe betrifft (Bst. c). Andererseits gelten nach Art. 5 Abs. 2 BGÖ als amtliche Dokumente auch solche, die durch einen einfachen elektronischen Vorgang aus aufgezeichneten Informationen erstellt werden können, welche die Anforderungen nach Absatz 1 Buchstaben b und c BGÖ erfüllen (sog. virtuelle Dokumente). Die Abgrenzung, wann ein Vorgang noch als einfach bezeichnet werden kann und wann nicht mehr, ist noch nicht abschliessend geklärt (Urteile des BVGer A-1784/2014 vom 30. April 2015 E. 4.1, A-1177/2014 vom 2. Februar 2015 E. 4.4.3 und A-931/2014 vom 9. Dezember 2014 E.8.3; ROBERT BÜHLER, in: Maurer-Lambrou/Blechta [Hrsg.], Datenschutzgesetz/Öffentlichkeitsgesetz, 3. Auflage 2014 [nachfolgend: BSK DSG/BGÖ], Art. 5 Rz. 18).

Die Vorinstanz stellte im Rahmen des vorinstanzlichen Verfahrens klar, dass keine Verzeichnisse existierten, welche die gesamten verlangten Informationen enthielten und für die Zusammenstellung einer kompletten Liste einige Stunden Aufwand anfallen würden. Ein erheblicher oder gar übermässiger Zeitbedarf sowie technische Schwierigkeiten für die Zusammentragung der dezentral vorhandenen elektronischen Informationen wurden dagegen nicht geltend gemacht. Entsprechend ist den erfragten Listen die Qualität von amtlichen Dokumenten im Sinne von Art. 5 Abs. 2 BGÖ zuzuschreiben.

3.4 Zusammenfassend ergibt sich, dass für die Auskunftserteilung im vorliegenden Fall die Bestimmungen des Öffentlichkeitsgesetzes anzuwenden sind. Nachfolgend ist zu prüfen, ob die Vorinstanz das Auskunftsgesuch des Beschwerdeführers zu Recht abgelehnt hat.

4.

4.1 Grundsätzlich hat jede Person das Recht, amtliche Dokumente einzusehen und von den Behörden Auskunft über den Inhalt amtlicher Dokumente zu erhalten (Art. 6 Abs. 1 BGÖ). Damit wird jeder Person ein generelles Recht auf Zugang zu amtlichen Dokumenten, über welche die Verwaltung verfügt, gewährt, ohne dass ein besonderes Interesse nachgewiesen werden müsste (BGE 136 II 399 E. 2.1, 133 II 209 E. 2.1; BVGE 2011/52 E. 3; statt vieler Urteil des BVGer A-4962/2012 vom 22. April 2013 E. 4 m.w.H.). Es obliegt entsprechend nicht mehr dem freien Ermessen der Behörden, ob sie Informationen oder Dokumente zugänglich machen wollen oder nicht. Der Zugang zu amtlichen Dokumenten kann jedoch eingeschränkt, aufgeschoben oder verweigert werden, wenn überwiegende private oder öffentliche Interessen an der Geheimhaltung einer Offenlegung entgegenstehen (Art. 7 BGÖ) oder wenn ein Ausnahmefall gemäss Art. 8 BGÖ vorliegt (s.a. BGE 136 II 399 E. 2).

4.2 Die privaten oder öffentlichen Interessen, welche eine Geheimhaltung rechtfertigen können, müssen das (öffentliche) Interesse am Zugang beziehungsweise an der Transparenz überwiegen. Das Gesetz nimmt die entsprechende Interessenabwägung selber vorweg, indem es in abschliessender Weise die verschiedenen Fälle überwiegender öffentlicher oder privater Interessen aufzählt (COTTIER/SCHWEIZER/WIDMER, in: Handkommentar BGÖ, Art. 7 Rz. 3). Die Beweislast zur Widerlegung der Vermutung des freien Zugangs, die durch das BGÖ aufgestellt wird, obliegt der Behörde (BVGE 2011/52 E. 6; Botschaft zum BGÖ, S. 2002; MAHON/GONIN, a.a.O., Art. 6 Rz. 11). Dabei hängt die Wirksamkeit dieser Ausnahmeklauseln einerseits davon ab, dass die Beeinträchtigung im Fall einer Offenlegung von einer gewissen Erheblichkeit sein muss, und andererseits, dass ein ernsthaftes Risiko bezüglich deren Eintritt besteht, mithin der Schaden nach dem üblichen Lauf der Dinge und mit hoher Wahrscheinlichkeit eintrifft. Wie dies bei Einschränkungen von Grundrechten im Allgemeinen der Fall ist, müssen die Ausnahmeklauseln restriktiv ausgelegt werden (vgl. BVGE 2013/50 E. 8.1 und 2011/52 E. 6; A-6291/2013 E. 7; Urs STEIMEN, BSK DSG/BGÖ, Art. 7 BGÖ Rz. 4; COTTIER/SCHWEIZER/WIDMER, a.a.O., Art. 7 Rz. 4). Der im BGÖ verankerte Mechanismus des Schutzes von Geheimhaltungsinteressen beruht damit auf dem Bestehen oder Nichtbestehen eines Schadensrisikos und mit Ausnahme von Art. 7 Abs. 2 BGÖ nicht auf einer eigentlichen Abwägung des Interesses der Verwaltung an der Geheimhaltung gegenüber jenem des Gesuchstellers auf Zugang zu den verlangten Dokumenten. Wenn die Behörde von einem ernsthaften Risiko

ausgehen muss, dass ein substanzieller Schaden einritt, muss das Dokument – ungeachtet der Legitimität der Gründe, aus denen die gesuchstellende Person um Zugang zur Information ersucht – geheim gehalten werden (STEIMEN, a.a.O., Art. 7 BGÖ Rz. 3; COTTIER/SCHWEIZER/WIDMER, a.a.O., Art. 7 Rz. 5).

4.3 Im Übrigen darf der Zugang aufgrund des Verhältnismässigkeitsprinzips nicht einfach verweigert werden, wenn ein verlangtes Dokument Informationen enthält, die nach dem Ausnahmekatalog von Art. 7 BGÖ nicht zugänglich sind. Vielmehr ist in diesem Fall ein eingeschränkter, das heisst teilweiser Zugang zu den Informationen im Dokument zu gewähren, welche nicht geheim zu halten sind (COTTIER/SCHWEIZER/WIDMER, a.a.O., Art. 7 Rz. 8; STEIMEN, a.a.O., Art. 7 Rz. 9 ff.).

5.
Nachfolgend ist für die in Frage stehenden Dokumente zu prüfen, ob der von der Vorinstanz in erster Linie geltend gemachte Ausnahmetatbestand von Art. 7 Abs. 1 Bst. b BGÖ nachgewiesen ist, wonach der Zugang zu amtlichen Dokumenten eingeschränkt, aufgeschoben oder verweigert wird, wenn durch seine Gewährung die zielkonforme Durchführung konkreter behördlicher Massnahmen beeinträchtigt würde. In einem weiteren Schritt ist gegebenenfalls zu prüfen, ob gestützt auf die Ausnahmebestimmungen die vollständige Verweigerung des Zugangs zu den einzelnen Dokumenten verhältnismässig ist.

5.1 Die Ausnahme vom Prinzip der Öffentlichkeit nach Art. 7 Abs. 1 Bst. b BGÖ kann dann angerufen werden, wenn durch die Zugänglichmachung bestimmter Informationen, die eine Massnahme vorbereiten, die betreffende Massnahme ihr Ziel mit hoher Wahrscheinlichkeit nicht mehr beziehungsweise nicht vollumfänglich erreichen würde. Geschützt sind insbesondere die Ermittlungen, die Inspektionen und die administrativen Überwachungen, mit denen sichergestellt werden soll, dass sich die Bürgerinnen und Bürger an das Gesetz halten (Botschaft zum BGÖ, BBl 2003 2009; COTTIER/SCHWEIZER/WIDMER, a.a.O., Art. 7 Rz. 23 ff.). Die Geheimhaltung der Informationen muss Bedingung für den Erfolg der entsprechenden Massnahme bilden (STEIMEN, a.a.O., Art. 7 BGÖ Rz. 19; Urteil des BVGer A-3122/2014 vom 24. November 2014 E. 4.2.2).

5.2 Im Post- und Fernmeldeverkehr, zu dem auch das Internet gehört, fallen Informationen an, die zur Aufklärung von schweren Verbrechen (vgl. Art. 269 ff. der Schweizerischen Strafprozessordnung vom 5. Oktober 2007

[StPO, SR 312.0]) erforderlich sein können. Die Vorinstanz führt auf Anordnung der Strafverfolgungsbehörden Post- und Fernmeldeüberwachungen durch. In letzterem Fall weist er die Anbieterinnen von Fernmeldediensten an, die für die Überwachung notwendigen Massnahmen zu treffen, nimmt von ihnen den umgeleiteten Fernmeldeverkehr der überwachten Person entgegen, zeichnet diesen auf und liefert der anordnenden Behörde die Dokumente und Datenträger aus. Die Vorinstanz betreibt dafür ein rund um die Uhr einsatzfähiges Verarbeitungszentrum. Nach der Übergabe, spätestens aber drei Monate nach der Einstellung der Überwachung, werden die gewonnenen Daten vernichtet. Des Weiteren sorgt die Vorinstanz auch für die Durchführung von Direktschaltungen (vgl. Art. 13 BÜPF sowie Art. 7 ff. der Verordnung vom 31. Oktober 2001 über die Überwachung des Post- und Fernmeldeverkehrs [VÜPF, SR 780.11]). Zur Bewältigung dieser Aufgaben bedient sich die Vorinstanz besonderer Softwareprodukte.

5.3

5.3.1 Die Vorinstanz gibt zu bedenken, dass mit der Kenntnis von Namen und Versionsnummern der von ihr eingesetzten Software ein Hindernis wegfallen würde, welches das Risiko unbefugten Eindringens in ihr IT-System herabsetzt. Ein erfolgreicher Angriff würde für die bearbeiteten Personendaten und die Strafverfolgung Folgen von nicht erdenklichem Ausmass nach sich ziehen. Da jedes Softwareprodukt Lücken, Schwachstellen oder "Exploits" (systematische Möglichkeit in der elektronischen Datenverarbeitung, Schwachstellen auszunutzen, die bei der Entwicklung eines Programms nicht berücksichtigt wurden) aufweise, die mit den nötigen Ressourcen aufgedeckt werden könnten, sei es zur Vermeidung von Angriffen unabdingbar, keine Informationen zur eingesetzten Software offenzulegen. Damit werde überdies auch die Gefahr minimiert, dass potenziell von Strafuntersuchungen Betroffene in Kenntnis der verwendeten Softwareprodukte Rückschlüsse auf die damit verbundenen Überwachungsmöglichkeiten ziehen und sich so der Strafverfolgung entziehen können.

5.3.2 Der Beschwerdeführer entgegnet, der vorinstanzlich vertretene Ansatz "Security by Obscurity" (Sicherheit durch Unklarheit) stelle kein Sicherheitskonzept dar. Vielmehr müsse die Sicherheit eines IT-Systems auch dann gewährleistet sein, wenn der Angreifer dessen Implementation und Komponenten kenne. Die Gefahr eines Angriffes ginge von Personen und Organisationen aus, welche ohnehin bereits über die ersuchten Informationen verfügten. Ebenso würden sich Personen mit den nötigen Fähigkeiten und Ressourcen ungeachtet der begehrten Informationen bereits

heute einer Überwachung entziehen können, womit die Effektivität der Überwachungsmassnahmen durch die Herausgabe der Informationen nicht beschlagen wäre. Die Öffentlichkeit der Informationen würde dagegen zu einer rascheren öffentlichen Diskussion von Sicherheitslücken führen und Risiken für überwachte Personen sowie Dritte minimieren.

5.4 Die Bekanntgabe von Namen und Versionsnummern der fraglichen Produkte soll laut Vorinstanz einerseits die Gefahr in sich bergen, dass gewisse Personen, in Verfolgung ihrer eigenen Interessen, Schwachstellen der verwendeten Software beziehungsweise Computersysteme aufspüren, in diese eindringen und entsprechenden Schaden anrichten. Dass Softwareprodukte unvermeidlich Angriffspunkte aufweisen, darf nach Auffassung des Bundesverwaltungsgerichtes als notorische Tatsache betrachtet werden und wird im Übrigen auch vom Beschwerdeführer nicht dementiert. Die Vorinstanz legt dabei überzeugend dar, dass ein IT-System grundsätzlich zwar auch bei Bekanntsein der ersuchten Informationen einem Hackerangriff standhalten sollte, die Geheimhaltung aber ein weiterer Schutzmechanismus darstellt, der von einem Angreifer zunächst überwunden werden müsste. Selbst wenn gewisse Akteure bereits über die fraglichen Informationen verfügen sollten, so erscheint es unter diesem Gesichtspunkt zur Verminderung des Risikos zielführend, eine breite Streuung der Daten zu vermeiden, um nicht weiteren Kreisen die Überwindung der Sicherheitsbarrieren zu erleichtern. Der erhobene Einwand des Beschwerdeführers, die breite öffentliche Diskussion über die Sicherheit der Softwareprodukte würde der Aufdeckung und zeitnahen Behebung von Sicherheitslücken dienen, ist dagegen nicht stichhaltig. Es ist der Vorinstanz beizupflichten, wenn sie die Gewährleistung der Sicherheit nicht an die breite Öffentlichkeit delegieren möchte, sondern auf die organisationsinterne Erkennung und Behebung von Mängeln setzt. Es ist davon auszugehen, dass sie dabei auf ausgewiesene Spezialisten zurückgreifen kann. Ein allfälliger Zusatznutzen durch Rückmeldungen aus spezialisierten und interessierten Kreisen der Öffentlichkeit vermöchte die Risiken des vorerwähnten Missbrauchs keinesfalls aufzuwiegen. In einer Zeit in der Computerkriminalität dem Alltag angehört und in stets neuer Form und Intensität auftritt, ist es lebensfremd anzunehmen, mit der Veröffentlichung der sensiblen Daten könne primär auf die wohlwollende Hilfeleistung der Bevölkerung und eine entsprechende Schadenminderung gezählt werden. Das kriminelle Potenzial und die damit verbundene Gefahr von Hackerangriffen dürfte weitaus grösser sein. Schliesslich leuchtet es ein, dass mit dem unerlaubten Eindringen in das Überwachungssystem der Vorinstanz eine Gefährdung der bearbeiteten Daten sowie der Überwachungsmassnahmen einhergehen

würde und ihr Ziel mit hoher Wahrscheinlichkeit nicht mehr beziehungsweise nicht mehr vollumfänglich erreicht werden könnte (vgl. E. 5.1).

5.5 Andererseits weist die Vorinstanz zurecht darauf hin, dass es bei einer Offenlegung der verlangten Informationen diversen Kreisen gelingen könnte, sich ein umfassendes Bild über die Ermittlungsmethodik und die technischen Möglichkeiten sowie die Grenzen der Überwachungen zu machen. Interessierten beziehungsweise betroffenen Personen würde damit die Möglichkeit geboten, auf nicht überwachbare Kommunikationskanäle auszuweichen, um sich einer Überwachung durch die Vorinstanz zu entziehen. Der Erfolg der Überwachungsmassnahmen würde somit auch insoweit infrage gestellt. Ein kleiner Teil der Zielpersonen mag bereits heute über das erforderliche Wissen verfügen. Die Vorinstanz spricht dabei jedoch zutreffend von einem üblichen Ermittlungsrisiko, das es von den Strafverfolgungsbehörden zu tragen gilt. Bei einer weiteren Verbreitung der Informationen sieht sie dagegen schweizweit das wichtige Instrument der Post- und Fernmeldeüberwachung zur Bekämpfung der Kriminalität und Gewährung der inneren Sicherheit gefährdet. Unabhängig des tatsächlich zu gewärtigenden Ausmasses der negativen Konsequenzen für die Strafverfolgung legt die Vorinstanz jedenfalls zurecht dar, dass die Kenntnis der konkret verwendeten Softwareprodukte ein wichtiger Schlüssel ist, um deren Anwendungsmöglichkeiten in Erfahrung zu bringen. Entsprechend ist von einer Korrelation zwischen der begehrten Bekanntgabe und den vorerwähnten negativen Auswirkungen auf den Erfolg von Überwachungsmassnahmen auszugehen. Auch der Beschwerdeführer bestätigt diesen Befund, wenn er sein Anliegen auch damit propagiert, dass es dem Einzelnen durch die Kenntnis der konkreten Fähigkeiten der Vorinstanz möglich sein soll, sich vor einer ungerechtfertigten Überwachung zu schützen.

5.6 Zusammenfassend ist nach Ansicht des Bundesverwaltungsgerichts nachvollziehbar dargetan, dass bei Gewährung des ersuchten Zugangs mit Beeinträchtigungen der Überwachungsmassnahmen der Vorinstanz zu rechnen ist, wobei diese einerseits von Hackerangriffen auf die IT-Systeme (E. 5.4) und andererseits von der adaptierten Verhaltensweise potenziell zu überwachender Zielpersonen (E. 5.5) ausgehen können.

5.7 Da die fraglichen Massnahmen ein wichtiges Instrument bei der Aufklärung von Straftaten darstellen (vgl. E. 5.2), steht mit den dargelegten Beeinträchtigungsformen nicht nur der Erfolg beziehungsweise die Wirksamkeit der einzelnen Massnahmen selbst, sondern der Strafverfolgung insgesamt auf dem Spiel. Angesichts dieser Auswirkungen, welche letztlich die

innere Sicherheit der Schweiz berühren, sowie der Tatsache, dass das Überwachungssystem der Vorinstanz das Kernstück ihrer Tätigkeit darstellt, ist von einem erheblichen Schadenspotenzial auszugehen.

Aufgrund der globalen, zeit- und ortsunabhängigen Bedrohung durch Computerkriminalität sowie der unterschiedlichen Angriffsflächen, die das Überwachungssystem bietet (vgl. E. 5.4 und 5.5), ist auch die Eintretenswahrscheinlichkeit als hoch zu erachten. Dies gilt umso mehr, als Behörden mit staatlichen Sicherheitsaufgaben speziell im Fokus von Cyberkriminellen stehen dürften. Da mit der Strafverfolgung und dem Ausfällen von Strafen überdies eine general- sowie spezialpräventive Wirkung angestrebt wird und vorliegend eine Einschränkung des Öffentlichkeitsprinzips dieser Funktion dienlich ist, wird auch der Zwecksetzung der Ausnahmebestimmung, ein gesetzeskonformes Verhalten der Bürger sicherzustellen, entsprochen. Im Ergebnis besteht kein Anlass, von der Einschätzung der Vorinstanz abzuweichen. In tatbestandlicher Hinsicht ist mithin für den Fall der Gewährung des begehrten Zugangs mit hoher Wahrscheinlichkeit von einer erheblichen Beeinträchtigung der zielkonformen Durchführung der Überwachungsmassnahmen auszugehen. Die Ausnahmebestimmung von Art. 7 Abs. 1 Bst. b BGÖ ist somit erfüllt.

6. Die Vorinstanz beruft sich zur Begründung ihres abschlägigen Entscheids ferner auf den Ausnahmetatbestand gemäss Art. 7 Abs. 1 Bst. c BGÖ. Demnach kann der Zugang unter anderem eingeschränkt oder verweigert werden, wenn durch die Einsicht die innere Sicherheit der Schweiz gefährdet werden kann.

6.1 Diese Bestimmung soll in erster Linie die Tätigkeit von Polizei, Zoll, Nachrichtendienst und der Armee schützen (Botschaft zum BGÖ, S. 2009). Massgeblich ist jedoch nicht die Abgrenzung nach den tätigen Behörden, sondern die Abgrenzung von gefährdeten Interessen und Rechtsgütern. Sicherheit ist hierbei sowohl als Unverletzlichkeit der Rechtsgüter der Einzelnen wie auch des Staates und seiner Einrichtungen sowie der Rechtsordnung insgesamt zu verstehen. Die Ausnahmebestimmung dient der Geheimhaltung von Massnahmen, die von der Regierung getroffen oder in Betracht gezogen werden, um die öffentliche Ordnung innerhalb des Landes aufrechtzuerhalten. Schutzbedürftig können auch Informationen über die Organisation, die Tätigkeit und Strategie von Behörden mit Sicherheitsaufgaben sein (STEIMEN, a.a.O., Art. 7 Rz. 21 f.). Allerdings muss auch bei

legitimen Sicherheitszwecken sorgfältig geprüft werden, ob die Offenlegung der verlangten Dokumente die öffentliche Sicherheit ernsthaft gefährden könnte (COTTIER/SCHWEIZER/WIDMER, a.a.O. Art. 7, Rz. 26, 28).

6.2 Wie bereits festgestellt wurde, besteht zwischen der zu erwartenden Beeinträchtigung von Überwachungsmassnahmen der Vorinstanz im Falle einer Gutheissung des Einsichtsbegehrens und einer effektiven Strafverfolgung ein enger Zusammenhang (vgl. E. 5.7). Kommt es zu Hackerangriffen auf das Überwachungssystem oder entziehen sich Zielpersonen der vorgesehenen Überwachung, werden die Strafverfolgungsbehörden eines wirksamen Instrumentes in der Kriminalitätsbekämpfung beraubt. Dies wiederum führte unweigerlich zu einer ernsthaften Gefährdung der inneren Sicherheit im vorerwähnten Sinne, weshalb die uneingeschränkte Geheimhaltung auch unter diesem Titel (Art. 7 Abs. 1 Bst. c BGÖ) gerechtfertigt ist.

7.
Da nach dem Gesagten die Ausnahmebestimmungen von Art. 7 Abs. 1 Bst. b und c BGÖ zur Anwendung gelangen, kann die Frage, ob zusätzlich auch die Ausnahme von Art. 7 Abs. 1 Bst. e BGÖ einschlägig ist, offen bleiben.

8.
Der Beschwerdeführer rügt ferner die pauschale, vollumfängliche Verweigerung der Herausgabe, ohne dass eine Differenzierung nach Funktion der Software getroffen worden sei. Die Vorinstanz verfalle damit der Willkür.

8.1 Diesen Einwand gilt es unter dem Gesichtspunkt der Verhältnismässigkeit zu prüfen. Es stellt sich die Frage, ob gestützt auf die Ausnahmebestimmung die vollständige Verweigerung des Zugangs zu sämtlichen Informationen verhältnismässig ist. Das Verhältnismässigkeitsprinzip verlangt, dass die von der Behörde gewählte Verwaltungsmassnahme für das Erreichen des Zieles geeignet, notwendig und für die Betroffenen zumutbar ist. Die Verwaltungsmassnahme darf nicht einschneidender sein als erforderlich und hat zu unterbleiben, wenn eine gleich geeignete, aber mildere Massnahme für den angestrebten Erfolg ausreichen würde (Urteile des BVGer A-3122/2014 vom 24. November 2014 E. 4.5 und A-3631/2009 vom 15. September 2009 E. 3.4.1; HÄFELIN/MÜLLER/UHLMANN, Allgemeines Verwaltungsrecht, 6. Auflage 2010, Rz. 581 ff.).

8.2 Nebst der unterlassenen funktionsbezogenen Unterscheidung, wie sie im Rechtsbegehren des Beschwerdeführers zum Ausdruck kommt, bemängelt Letzterer die mangelnde Abgrenzung von sicherheitskritischer Software zu solcher mit Hilfsfunktion (insbesondere Speicherung, Transport oder Anzeige). Ebenso fehle die Trennung von Softwareprodukten mit Kontakt zu öffentlichen Fernmeldenetzen und solchen, die ausschliesslich in geschützter Umgebung Anwendung fänden. Dieser Argumentation folgend, vertritt er für den Fall, dass die Herausgabe dennoch eine Gefährdung durch Angriffe mit sich bringen sollte, den Standpunkt, es rechtfertige sich höchstens die Verweigerung bezüglich der Softwareprodukte zur Absicherung der technischen Infrastruktur (vgl. Begehren Ziff. 1 e). Wenn überdies die Effektivität von Überwachungsmassnahmen beeinträchtigt sein sollte, so beträfe dies lediglich die Software zur Ausleitung, Erfassung, Ausscheidung, Auswertung sowie Aufbereitung von Daten (vgl. Begehren Ziff. 1 a und b), nicht jedoch die übrigen Produkte.

8.3 Die Vorinstanz wendet dagegen ein, sämtliche Software- und Hardwarekomponenten stellten zusammen ein funktionsfähiges und nicht kompromittierbares Überwachungssystem in ein und demselben Sicherheitskontext dar, weshalb eine getrennte Beurteilung nicht möglich sei. Gerade auch die Softwareapplikationen zur Speicherung, Transport und Anzeige von Personendaten, welchen der Beschwerdeführer Hilfsfunktion zuschreibt, würden besonders sicherheitskritische Bereiche darstellen. Die Vorinstanz zeigt damit nachvollziehbar auf, dass auch mit der Bekanntgabe einzelner Softwarekategorien als Element des gesamten Überwachungssystems, die Sicherheit des Gesamtsystems auf dem Spiel steht und nur eine umfassende Geheimhaltung die unbeeinträchtigte Wahrnehmung der Überwachungstätigkeit garantieren kann. Es besteht kein Anlass, an dieser Darstellung zu zweifeln. Eine teilweise Gewährung der gewünschten Auskunft ist daher ausgeschlossen. Immerhin sah sich die Vorinstanz im Rahmen des vorinstanzlichen Verfahrens in der Lage, die gesamte Standardsoftware offenzulegen, welche auf ihrer Büroautomation eingesetzt wird und nicht explizit mit ihrer Kerntätigkeit zusammenhängt, sondern grösstenteils dem Bundesstandard entspricht. Ferner verweist sie auch auf ihre Bereitschaft, interessierten oder besorgten Privatpersonen so weit als möglich Rede und Antwort zu stehen. Auf ihrer Website (<www.li.admin.ch>) stellt sie überdies Statistiken zur Anzahl Überwachungsaufträge und Auskünfte je Kanton und Jahr sowie weitere Dokumentationen zur Verfügung. Mit der Verweigerung weitergehender Informationen wurde der Grundsatz der Verhältnismässigkeit gewahrt. Der in diesem Zusammenhang erhobene Vorwurf der Willkür verfängt nicht.

9.

Schliesslich ist auf den Einwand einzugehen, die Verfügung verletze die Informationsfreiheit (Art. 16 Abs. 3 BV) und die freie politische Willensbildung (Art. 34 Abs. 2 BV). Die ins Feld geführten Grundrechte erfuhren mit der Einführung des BGÖ eine Stärkung, da die Bundesverwaltung neu dem Grundsatz der Öffentlichkeit unterstellt wurde (Art. 6 Abs. 1 BGÖ). Zur Wahrung höherwertiger öffentlicher und privater Interessen sehen Art. 7 BGÖ und Art. 8 BGÖ für bestimmte Fälle eine Einschränkung dieses Prinzips vor. Mit diesen Ausnahmebestimmungen liegen formell-gesetzliche Grundlagen gemäss Art. 36 Abs. 1 BV vor, welche eine Grundrechtseinschränkung rechtfertigen können. Indem vorliegend die Ausnahmetatbestände nach Art. 7 Abs. 1 Bst. b und c BGÖ erfüllt sind (E. 7) und die Einschränkung überdies durch das öffentliche Interesse nach innerer Sicherheit gerechtfertigt ist sowie verhältnismässig ausfällt, ist die vorinstanzliche Verfügung entgegen der Darstellung des Beschwerdeführers nicht in Verletzung von Grundrechten ergangen. Die Beschwerde erweist sich folglich als unbegründet und ist abzuweisen.

10.

Bei diesem Verfahrensausgang gilt der Beschwerdeführer als unterliegend, weshalb er in Anwendung von Art. 63 Abs. 1 VwVG die Verfahrenskosten zu tragen hat. Diese sind auf Fr. 1'500.00 festzusetzen (Art. 1 ff. des Reglements vom 21. Februar 2008 über die Kosten und Entschädigungen vor dem Bundesverwaltungsgericht [VGKE, SR 173.320.2]). Der einbezahlte Kostenvorschuss wird zur Bezahlung der Verfahrenskosten verwendet. Dem unterliegenden Beschwerdeführer steht keine Parteientschädigung zu (Art. 64 VwVG i.V.m. Art. 7 ff. VGKE).

Demnach erkennt das Bundesverwaltungsgericht:

1.
Die Beschwerde wird abgewiesen.

2.
Die Verfahrenskosten von Fr. 1'500.00 werden dem Beschwerdeführer auferlegt. Der einbezahlte Kostenvorschuss wird zur Bezahlung der Verfahrenskosten verwendet.

3.
Es wird keine Parteientschädigung zugesprochen.

4.
Dieses Urteil geht an:

– den Beschwerdeführer (Gerichtsurkunde)
– die Vorinstanz (Einschreiben)
– das Generalsekretariat des Eidgenössischen Justiz- und Polizeidepartements EJPD (Gerichtsurkunde)
– den EDÖB (zur Kenntnis)

Der vorsitzende Richter:	Der Gerichtsschreiber:
Jürg Steiger	Matthias Stoffel

Rechtsmittelbelehrung:

Gegen diesen Entscheid kann innert 30 Tagen nach Eröffnung beim Bundesgericht, 1000 Lausanne 14, Beschwerde in öffentlich-rechtlichen Angelegenheiten geführt werden, sofern die Voraussetzungen gemäss Art. 82 ff., 90 ff. und 100 BGG gegeben sind. Die Rechtsschrift ist in einer Amtssprache abzufassen und hat die Begehren, deren Begründung mit Angabe der Beweismittel und die Unterschrift zu enthalten. Der angefochtene Entscheid und die Beweismittel sind, soweit sie der Beschwerdeführer in Händen hat, beizulegen (Art. 42 BGG).

Versand: