BESCHLUSS (GASP) 2021/1026 DES RATES

vom 21. Juni 2021

zur Unterstützung des Programms für Cybersicherheit und -abwehrfähigkeit sowie für Informationssicherung der Organisation für das Verbot chemischer Waffen (OVCW) im Rahmen der Umsetzung der EU-Strategie gegen die Verbreitung von Massenvernichtungswaffen

DER RAT DER EUROPÄISCHEN UNION —

gestützt auf den Vertrag über die Europäische Union, insbesondere auf Artikel 28 Absatz 1 und Artikel 31 Absatz 1,

auf Vorschlag des Hohen Vertreters der Union für Außen- und Sicherheitspolitik,

in Erwägung nachstehender Gründe:

(1) Am 12. Dezember 2003 hat der Europäische Rat die Strategie der EU gegen die Verbreitung von Massenvernichtungswaffen (im Folgenden „EU-Strategie“) angenommen, deren Kapitel III eine Reihe von Maßnahmen zur Bekämpfung der Verbreitung solcher Waffen enthält.

(2) In der EU-Strategie wird die maßgebliche Rolle hervorgehoben, die dem Übereinkommen über das Verbot der Entwicklung, Herstellung, Lagerung und des Einsatzes chemischer Waffen und über die Vernichtung solcher Waffen (CWÜ) und der Organisation für das Verbot chemischer Waffen (OVCW) bei der Schaffung einer Welt ohne Chemiewaffen zukommt. Die Ziele der EU-Strategie ergänzen diejenigen, die von der OVCW im Rahmen ihrer Zuständigkeit für die Durchführung des CWÜ verfolgt werden.

(3) Am 22. November 2004 hat der Rat die Gemeinsame Aktion 2004/797/GASP ([1]) zur Unterstützung der Maßnahmen der OVCW angenommen. Auf diese Gemeinsame Aktion folgte nach Ablauf ihrer Geltungsdauer die Gemeinsame Aktion 2005/913/GASP des Rates ([2]), auf die wiederum die Gemeinsame Aktion 2007/185/GASP des Rates ([3]) folgte.

Der Gemeinsamen Aktion 2007/185/GASP folgten die Beschlüsse 2009/569/GASP ([4]), 2012/166/GASP ([5]), 2013/726/GASP ([6]), (GASP) 2015/259 ([7]), (GASP) 2017/2302 ([8]), (GASP) 2017/2303 ([9]) und (GASP) 2019/538 ([10]) des Rates.

([1]) Gemeinsame Aktion 2004/797/GASP des Rates vom 22. November 2004 zur Unterstützung der Maßnahmen der OVCW im Rahmen der Umsetzung der Strategie der EU gegen die Verbreitung von Massenvernichtungswaffen (ABl. L 349 vom 25.11.2004, S. 63).

([2]) Gemeinsame Aktion 2005/913/GASP des Rates vom 12. Dezember 2005 zur Unterstützung der Maßnahmen der OVCW im Rahmen der Umsetzung der Strategie der EU gegen die Verbreitung von Massenvernichtungswaffen (ABl. L 331 vom 17.12.2005, S. 34).

([3]) Gemeinsame Aktion 2007/185/GASP des Rates vom 19. März 2007 zur Unterstützung der Maßnahmen der OVCW im Rahmen der Umsetzung der Strategie der EU gegen die Verbreitung von Massenvernichtungswaffen (ABl. L 85 vom 27.3.2007, S. 10).

([4]) Beschluss 2009/569/GASP des Rates vom 27. Juli 2009 zur Unterstützung der Maßnahmen der OVCW im Rahmen der Umsetzung der Strategie der EU gegen die Verbreitung von Massenvernichtungswaffen (ABl. L 197 vom 29.7.2009, S. 96).

([5]) Beschluss 2012/166/GASP des Rates vom 23. März 2012 zur Unterstützung von Maßnahmen der Organisation für das Verbot chemischer Waffen (OVCW) im Rahmen der Umsetzung der Strategie der EU gegen die Verbreitung von Massenvernichtungswaffen (ABl. L 87 vom 24.3.2012, S. 49).

([6]) Beschluss 2013/726/GASP des Rates vom 9. Dezember 2013 zur Unterstützung der Resolution 2118 (2013) des Sicherheitsrats der Vereinten Nationen und des Beschlusses EC-M-33/Dec 1 des Exekutivrats der OVCW im Rahmen der Umsetzung der Strategie der EU gegen die Verbreitung von Massenvernichtungswaffen (ABl. L 329 vom 10.12.2013, S. 41).

([7]) Beschluss (GASP) 2015/259 des Rates vom 17. Februar 2015 zur Unterstützung von Maßnahmen der Organisation für das Verbot chemischer Waffen (OVCW) im Rahmen der Umsetzung der Strategie der EU gegen die Verbreitung von Massenvernichtungswaffen (ABl. L 43 vom 18.2.2015, S. 14).

([8]) Beschluss (GASP) 2017/2302 des Rates vom 12. Dezember 2017 zur Unterstützung der Tätigkeiten der OVCW im Hinblick auf die Unterstützung von Sanierungsmaßnahmen in der ehemaligen Lagerstätte für chemische Waffen in Libyen im Rahmen der Umsetzung der Strategie der EU gegen die Verbreitung von Massenvernichtungswaffen (ABl. L 329 vom 13.12.2017, S. 49).

([9]) Beschluss (GASP) 2017/2303 des Rates vom 12. Dezember 2017 zur Unterstützung der weiteren Umsetzung der Resolution 2118 (2013) des Sicherheitsrates der Vereinten Nationen und des Beschlusses EC-M-33/DEC.1 des Exekutivrates OVCW über die Vernichtung der syrischen Chemiewaffen im Rahmen der Umsetzung der Strategie der EU gegen die Verbreitung von Massenvernichtungswaffen (ABl. L 329 vom 13.12.2017, S. 55).

([10]) Beschluss (GASP) 2019/538 des Rates vom 1. April 2019 zur Unterstützung von Maßnahmen der Organisation für das Verbot chemischer Waffen (OVCW) im Rahmen der Umsetzung der Strategie der EU gegen die Verbreitung von Massenvernichtungswaffen (ABl. L 93 vom 2.4.2019, S. 3).

(4) Im Rahmen der aktiven Umsetzung des Kapitels III der EU-Strategie ist die Fortführung dieser intensiven und gezielten Unterstützung der Union für die OVCW erforderlich.

(5) Es bedarf weiterer Unterstützung der Union für das Programm für Cybersicherheit und -abwehrfähigkeit sowie für Informationssicherung der OVCW, mit dem die Kapazität der OVCW verbessert werden soll, um ein angemessenes Maß an Cybersicherheit und -abwehrfähigkeit zur Bewältigung aktueller und sich abzeichnender Herausforderungen im Zusammenhang mit der Cybersicherheit aufrechtzuerhalten —

HAT FOLGENDEN BESCHLUSS ERLASSEN:

Artikel 1

(1) Zur sofortigen praktischen Anwendung bestimmter Bestandteile der EU-Strategie unterstützt die Union ein Projekt der OVCW mit folgenden Zielen:

— Ausbau der IKT-Infrastruktur entsprechend dem institutionellen Rahmen der OVCW für die Betriebskontinuität mit besonderem Schwerpunkt auf Abwehrfähigkeit; und

— Gewährleistung der Governance für den privilegierten Zugriff sowie der physischen, logischen und kryptografischen Informationsverwaltung und -trennung für alle strategischen Netze und Missionsnetze der OVCW.

(2) Im Kontext des Absatzes 1 handelt es sich bei den von der Union unterstützten Maßnahmen des Projekts der OVCW, die im Einklang mit den Maßnahmen gemäß Kapitel III der EU-Strategie stehen, um folgende Maßnahmen:

— Schaffung günstiger Rahmenbedingungen für laufende Bemühungen um Cybersicherheit und -abwehrfähigkeit im Rahmen von OVCW-Operationen an mehreren Standorten;

— Entwicklung einer maßgeschneiderten Lösung für die lokale oder cloud-gestützte Integration und Konfiguration von Systemen mit den IKT-Systemen der OVCW und von Lösungen für die Verwaltung des privilegierten Zugriffs (Privileged Access Management/PAM); und

— Initiierung und Erprobung von PAM-Lösungen.

(3) Eine ausführliche Beschreibung der in Absatz 2 genannten, von der Union unterstützten Maßnahmen der OVCW ist im Anhang enthalten.

Artikel 2

(1) Für die Durchführung dieses Beschlusses ist der Hohe Vertreter der Union für Außen- und Sicherheitspolitik (im Folgenden „Hoher Vertreter“) zuständig.

(2) Die technische Durchführung des in Artikel 1 genannten Projekts obliegt dem Technischen Sekretariat der OVCW (im Folgenden „Technisches Sekretariat“). Es nimmt diese Aufgabe unter der Verantwortung und Aufsicht des Hohen Vertreters wahr. Dazu trifft der Hohe Vertreter die erforderlichen Vereinbarungen mit dem Technischen Sekretariat.

Artikel 3

(1) Der finanzielle Bezugsrahmen für die Durchführung des in Artikel 1 genannten Projekts beträgt 2 151 823 EUR.

(2) Die mit dem Betrag nach Absatz 1 finanzierten Ausgaben werden entsprechend den für den Gesamthaushaltsplan der Union geltenden Verfahren und Vorschriften verwaltet.

(3) Die Kommission beaufsichtigt die ordnungsgemäße Verwaltung der in Absatz 2 genannten Ausgaben. Hierfür schließt sie das erforderliche Abkommen mit dem Technischen Sekretariat. In diesem Abkommen wird festgehalten, dass das Technische Sekretariat zu gewährleisten hat, dass dem Beitrag der Union die seinem Umfang entsprechende öffentliche Beachtung zuteilwird, und anzugeben hat, mit welchen Maßnahmen die Entwicklung von Synergien erleichtert werden kann und Doppelarbeit vermieden werden kann.

(4) Die Kommission ist bestrebt, das in Absatz 3 genannte Abkommen so bald wie möglich nach dem Inkrafttreten dieses Beschlusses zu schließen. Sie unterrichtet den Rat über etwaige Schwierigkeiten dabei und teilt ihm den Zeitpunkt mit, zu dem das Abkommen geschlossen wird.

Artikel 4

Der Hohe Vertreter unterrichtet den Rat auf der Grundlage regelmäßiger, vom Technischen Sekretariat erstellter Berichte über die Durchführung dieses Beschlusses. Die Berichte des Hohen Vertreters bilden die Grundlage für die Bewertung durch den Rat. Die Kommission liefert Informationen über die finanziellen Aspekte des in Artikel 1 genannten Projekts.

Artikel 5

(1) Dieser Beschluss tritt am Tag seiner Annahme in Kraft.

(2) Die Geltungsdauer dieses Beschlusses endet 24 Monate nach Abschluss des in Artikel 3 Absatz 3 genannten Abkommens. Sie endet jedoch sechs Monate nach dem Inkrafttreten des Beschlusses, falls das Abkommen nicht bis zu diesem Zeitpunkt geschlossen worden ist.

Geschehen zu Luxemburg am 21. Juni 2021.

Im Namen des Rates
Der Präsident
J. BORRELL FONTELLES

ANHANG

PROJEKTDOKUMENT

1. Hintergrund

Die OVCW ist verpflichtet, eine Infrastruktur zu unterhalten, die eine den Klassifizierungen des privilegierten Zugriffs, geeigneten Abwicklungsprozessen und bestehenden Bedrohungen entsprechende Informationshoheit ermöglicht und gleichzeitig gegen sich abzeichnende Risiken gewappnet ist. Die OVCW ist nach wie vor ständig mit schwerwiegenden und sich abzeichnenden Risiken in Bezug auf die Cybersicherheit und Cyberabwehrfähigkeit konfrontiert. Die OVCW ist Angriffsziel hochqualifizierter, sehr gut ausgestatteter und hochmotivierter Akteure. Von diesen Akteuren gehen nach wie vor häufige Angriffe auf die Vertraulichkeit und Integrität der Informationsressourcen und Infrastrukturanlagen der OVCW aus. Um den Bedenken Rechnung zu tragen, die durch jüngste Cyberangriffe, aktuelle politische Erwägungen und die COVID-19-Krise hervorgehoben wurden, und die besonderen Anforderungen zu berücksichtigen, die sich aus der Art der Arbeit der OVCW hinsichtlich der Erfüllung des Mandats des CWÜ ergeben, müssen unbedingt entscheidende Investitionen in technische Fähigkeiten vorgenommen werden.

Im Rahmen des Sonderfonds der OVCW für Cybersicherheit, Betriebskontinuität und physische Infrastruktursicherheit hat die OVCW 47 Maßnahmen zur Bewältigung der in jüngster Zeit aufgetretenen Herausforderungen im Bereich der Cybersicherheit für ihr Programm für Cybersicherheit und -abwehrfähigkeit sowie für Informationssicherung (im Folgenden „OVCW-Programm“) konzipiert. Das OVCW-Programm orientiert sich an den bewährten Verfahren, die von Einrichtungen wie der Agentur der Europäischen Union für Cybersicherheit (ENISA) gefördert werden, oder verwendet Konzepte im Zusammenhang mit der europäischen Richtlinie über die Sicherheit von Netz- und Informationssystemen (NIS) in den Bereichen Telekommunikation und Verteidigung. Insgesamt deckt das OVCW-Programm folgende Themenbereiche ab: Netze für Verschlusssachen und andere Netze, Politik und Governance, Aufdeckung und Reaktion, Betrieb und Wartung sowie Telekommunikation. Grundsätzlich ist das OVCW-Programm so konzipiert, dass die OVCW in die Lage versetzt werden soll, sehr gut ausgestattete und/oder staatlich finanzierte Angreifer an der Erreichung ihrer Ziele zu hindern und von externen und internen Bedrohungen ausgehenden Risiken sowohl aus menschlicher als auch aus technischer Sicht zu mindern. Die Unterstützung der Union ist als Projekt mit drei Maßnahmen strukturiert, das zwei der 47 Maßnahmen des OVCW-Programms entspricht.

2. Zweck des Projekts

Übergeordnetes Ziel des Projekts ist es sicherzustellen, dass das OVCW-Sekretariat die Kapazität besitzt, um ein angemessenes Maß an Cybersicherheit und -abwehrfähigkeit zur Bewältigung wiederkehrender und sich abzeichnender Verteidigungsherausforderungen im Zusammenhang mit der Cybersicherheit in den Hauptquartieren und zugehörigen Einrichtungen der OVCW aufrechtzuerhalten, damit die OVCW ihr Mandat erfüllen und das CWÜ wirksam umgesetzt werden kann.

3. Ziele

— Ausbau der IKT-Infrastruktur im Einklang mit dem institutionellen Rahmen der OVCW für die Betriebskontinuität, mit besonderem Schwerpunkt auf Abwehrfähigkeit;

— Gewährleistung der Governance des privilegierten Zugriffs sowie der physischen, logischen und kryptografischen Informationsverwaltung und -trennung für alle strategischen Netze und Missionsnetze.

4. Ergebnisse

Folgende Ergebnisse, zu denen das Projekt beiträgt, werden erwartet:

— Sicherstellung, dass die IKT-Ausrüstung und die IKT-Dienste eine robuste Systemzuverlässigkeit (hybride/geografische Redundanz) bieten und eine bessere Verfügbarkeit von IKT-Systemen und -Diensten zur Unterstützung der Betriebskontinuität erleichtern;

— Minimierung der Fähigkeit jedes einzelnen Faktors oder einzelnen Person, der Vertraulichkeit und Integrität von Informationen oder Systemen innerhalb der OVCW zu schaden.

5. Maßnahmen

5.1. Maßnahme 1 — Schaffung günstiger Rahmenbedingungen für laufende Bemühungen um Cybersicherheit und -abwehrfähigkeit im Rahmen von OVCW-Operationen an mehreren Standorten

Diese Maßnahme zielt darauf ab, günstige Rahmenbedingungen für eine reibungslose Umsetzung der Betriebskontinuitätsplanung der OVCW im Zusammenhang mit Cybersicherheit und -abwehrfähigkeit zu schaffen. Dies wird durch die Verbesserung der Infrastruktur erreicht- eine neue Architektur und/oder Archivierung für die Betriebskontinuität der OVCW über mehrere Standorte hinweg. Außerdem soll die Integration der Governance des privilegierten Zugriffs in die Verfahren der Betriebskontinuitätsplanung und -reaktion noch stärker erleichtert und unterstützt werden.

5.2. Maßnahme 2 — Entwicklung einer maßgeschneiderten Lösung für die lokale und cloud-gestützte Integration und Konfiguration von Systemen mit den IKT-Systemen der OVCW und Entwicklung von Lösungen für die Verwaltung des privilegierten Zugriffs (Privileged Access Management/PAM)

Im Mittelpunkt dieser Maßnahme steht die Umsetzung der günstigen Rahmenbedingungen in ein maßgeschneidertes Konzept für die lokale und die cloud-gestützte Integration und Konfiguration von Systemen mit den IKT-Systemen der OVCW und den PAM-Lösungen. Dies dürfte die Effizienz der Infrastruktur der IKT-Systeme steigern und zur Entwicklung eines integrierten PAM-Systems für kritische Anlagen führen, das Abschreckung und Aufdeckung ermöglicht und angemessene Fähigkeiten zur Bedrohungssuche verfügt.

5.3. Maßnahme 3 — Initiierung und Erprobung von PAM-Lösungen

Diese Maßnahme baut auf der geschaffenen Infrastruktur und den PAM-Lösungen auf, die konzipiert wurden, um die Integration und Konfiguration von der Theorie in die Praxis umzusetzen. Die Systeme müssen kartiert, profiliert und in bestehende Systeme eingebettet werden, wobei die damit verbundenen politischen und menschlichen Faktoren zu berücksichtigen sind. Danach findet eine gründliche Erprobung während der Umsetzung und über einen gewissen Zeitraum hinweg statt, um die Robustheit des Systems zu überprüfen und abzusichern (alle neuen Systeme verfügen über eine starke Authentifizierung für Nutzer und Geräte, über eine angemessene Klassifizierung und einen angemessenen Schutz der Informationen und über ein fortschrittliches System zur Vermeidung von Datenverlusten), wodurch das OVCW-Sekretariat in die Lage versetzt wird, Lücken zu erkennen und weitestmöglich Abhilfe zu schaffen.

6. Laufzeit

Die geschätzte Gesamtlaufzeit der im Rahmen dieses Projekts finanzierten Umsetzung wird voraussichtlich 24 Monate betragen.

7. Begünstigte

Begünstigte des Projekts sind das Personal des Technischen Sekretariats der OVCW, politische Entscheidungsgremien, nachgeordnete Stellen und die Interessenträger des CWÜ einschließlich der Vertragsstaaten.

8. Öffentlichkeitswirkung für die EU

Die OVCW ergreift im Rahmen angemessener Sicherheitserwägungen alle geeigneten Maßnahmen, um öffentlich bekannt zu machen, dass dieses Projekt von der Union finanziert wird.