ANTWORTEN DER EUROPÄISCHEN KOMMISSION

AUF DEN SONDERBERICHT DES EUROPÄISCHEN RECHNUNGSHOFES

Cybersicherheit: Organe, Einrichtungen und sonstige Stellen der EU sind im Allgemeinen nicht ausreichend gegen Bedrohungen gewappnet

Inhalt

Dieses Dokument enthält die Antworten der Europäischen Kommission auf die Bemerkungen in einem Sonderbericht des Europäischen Rechnungshofes gemäß Artikel 259 der Haushaltsordnung und wird zusammen mit dem Sonderbericht veröffentlicht.

I. DIE ANTWORTEN DER KOMMISSION ZUSAMMENGEFASST

a) Allgemeine Einleitung

Die Cybersicherheit ist zu einer der wichtigsten politischen und operativen Prioritäten der Europäischen Kommission geworden. Die COVID-19-Krise hat die Abhängigkeit der EU von digitalen Diensten (Cloud-Computing, mobile Geräte, künstliche Intelligenz) noch verstärkt. In den letzten zwei Jahren hat die EU eine massive Verlagerung hin zur Telearbeit erlebt. Das bedeutet, dass sowohl die Cyberkriminalität als auch die Cyberspionage, die beiden Hauptbedrohungen für die Organe, Einrichtungen und sonstigen Stellen der Europäischen Union (im Folgenden „EU-OESS"), nun auch in großem Umfang online stattfinden. Die Kommission ist sich dieser Entwicklung bewusst. Sie hat im Bereich der Cybersicherheit eine konsequente und entschlossene Führungsposition eingenommen. Mit dem 2019 in Kraft getretenen Rechtsakt zur Cybersicherheit wurde u. a. das Mandat der Agentur der Europäischen Union für Cybersicherheit (ENISA) erweitert und auf eine dauerhafte Grundlage gestellt. Mit diesem Rechtsakt wurde auch eine formelle Zusammenarbeit zwischen der ENISA und dem CERT-EU (dem IT-Notfallteam zur Unterstützung der EU-OESS) begründet. Im Jahr 2020 schlug die Kommission eine Erweiterung der Richtlinie zur Netz- und Informationssicherheit (im Folgenden „NIS-Richtlinie") vor, die demnächst vom Gesetzgeber verabschiedet wird.

Im Rahmen der Cybersicherheitsstrategie 2020 wurden auch drei Maßnahmen für die Cybersicherheit der EU-OESS festgelegt. Die Kommission kündigte eine Verordnung über die Informationssicherheit in den Organen, Einrichtungen und sonstigen Stellen der EU und eine Verordnung über gemeinsame Cybersicherheitsvorschriften für die Organe, Einrichtungen und sonstigen Stellen der EU an und verwies auf ihre Absicht, eine neue Rechtsgrundlage für das CERT-EU zu schaffen, um sein Mandat und seine Mittelausstattung zu stärken, damit es angesichts der zunehmenden Bedrohungen, Risiken und Vorfälle angemessen ausgerüstet ist.

Die Ausarbeitung dieser Vorschläge ist weit fortgeschritten. Obwohl sie noch nicht vom Kollegium angenommen wurden, werden sie voraussichtlich im ersten Quartal 2022 angenommen. Wichtige Fragen, die in dieser Vorbereitungsphase zwischen den Einrichtungen erörtert wurden, betreffen die Rechtsgrundlage des Vorschlags sowie die Haushaltskapazität aller EU-OESS, um die Anforderungen sowohl in Bezug auf die Finanzierung ihrer eigenen Cybersicherheitsbedürfnisse als auch in Bezug auf die Beschaffung der erforderlichen Mittel zur Unterstützung des CERT-EU und des Haushalts sowie insbesondere der Personalmittel zu erfüllen.

Die EU-OESS sind in Bezug auf die Cybersicherheit unterschiedlich gut gewappnet. Mehrere EU-OESS sind in Bezug auf die Cybersicherheit sehr gut vorbereitet und sollten weiterhin eine Vorreiterrolle einnehmen, indem sie Fortschritte und weitere Verbesserungen im gesamten Cybersicherheitsbereich anregen und bewirken. Zur Erzielung messbarer Fortschritte ist es wichtig, die unterschiedlichen Reifegrade der EU-OESS anzuerkennen und Prioritäten zu setzen. Dabei sollten die Verbesserungsmaßnahmen in erster Linie auf diejenigen EU-OESS ausgerichtet werden, bei denen die festgestellten Lücken die größten Risiken mit sich bringen.

b) Der Standpunkt der Kommission zu den wichtigsten Bemerkungen und Empfehlungen des EuRH

Die Kommission begrüßt den Bericht des EuRH über die Cybersicherheit der EU-OESS. Sie stellt fest, dass die Bedeutung eines gemeinsamen Rechtsrahmens für die Informations- und Cybersicherheit in den EU-OESS zur Erhöhung des allgemeinen Niveaus der Cybersicherheit in dem Bericht unterstrichen wird. Die Kommission stellt fest, dass die wichtigsten Bemerkungen und Empfehlungen des EuRH nicht auf die operative Cybersicherheit der Kommission an sich abzielen, sondern auf die politische Rolle der Kommission bei der Ausarbeitung von Vorschlägen für Rechtsvorschriften zur Erhöhung der Reife der EU-OESS im Bereich der Cybersicherheit.

In den künftigen Verordnungen über die Informationssicherheit in den Organen, Einrichtungen und sonstigen Stellen der EU und die gemeinsamen Cybersicherheitsvorschriften für die Organe, Einrichtungen und sonstigen Stellen der EU werden die gemeinsamen Regeln für die Erreichung eines hohen Niveaus der Informations- und Cybersicherheit festgelegt, aber die Umsetzung der Verordnungen im organisatorischen und operativen Kontext der einzelnen EU-OESS (insbesondere ihre Bedrohungs- und Risikoprofile) wird weiterhin eine Aufgabe sein, die von den EU-OESS eigenständig übernommen wird. Mit der vorgeschlagenen Verordnung über die Cybersicherheit werden Verfahren zur Einhaltung der Vorschriften geschaffen, die dem Ziel und dem Anwendungsbereich der neuen Vorschriften angemessen sind, ohne die Autonomie der EU-OESS zu beeinträchtigen.

Die Kommission führt derzeit den Vorsitz der Untergruppe „Cybersicherheit“ des Interinstitutionellen Ausschusses für den digitalen Wandel (ICDT); dabei handelt es sich um ein turnusmäßiges Mandat (für einen Zeitraum von bis zu zwei Jahren). Es wird darauf hingewiesen, dass für die Arbeit der Untergruppe keine eigenen Ressourcen bereitgestellt werden: Die Teilnehmer unternehmen alle Maßnahmen nach besten Kräften und auf freiwilliger Basis.

Die Kommission befürwortet die allgemeine Idee, die Mittelausstattung und das Mandat des CERT-EU zu stärken.

In diesem Sinne unterstützt die Kommission die wichtigsten Feststellungen und Empfehlungen des Berichts. Der detaillierte Standpunkt der Kommission wird in den zusätzlichen Bemerkungen in Abschnitt III erläutert. Die Kommission akzeptiert die Empfehlungen 1a–1g und 2a–2c.

c) Einschlägige aktuelle Entwicklungen und nächste Schritte

Eine formelle Konsultation auf der Ebene der Generaldirektoren der EU-OESS zu den konsolidierten Entwürfen der beiden Verordnungen (Informationssicherheit, Cybersicherheit) ist abgeschlossen, und die Bewertung der eingegangenen Rückmeldungen ist im Gange, bevor das Paket vervollständigt und vom Kollegium im ersten Quartal 2022 angenommen wird.

II. ANTWORTEN DER KOMMISSION AUF DIE WICHTIGSTEN BEMERKUNGEN DES EUROPÄISCHEN RECHNUNGSHOFES

1. Reifegrad der Cybersicherheit der EU-OESS

Die Kommission stimmt zu, dass es wichtig ist, bei der Betrachtung der Höhe der Ausgaben der EU-OESS für die Cybersicherheit die Bedrohungen und Risiken zu berücksichtigen.

Auch im Bereich der Humanressourcen wird die Stabilität des Personalbestands der EU-OESS durch eine Reihe von Faktoren beeinflusst. Der Markt für die Einstellung von spezialisierten Cybersicherheitsexperten wird immer komplexer. In vielen Fällen sind die Personalvorschriften nicht an spezialisierte Profile angepasst (Einstellung, Laufbahnentwicklung, Ausbildung). Darüber hinaus bedeutet der allgemeine Druck in Bezug auf den Personalbestand in den EU-OESS durch die Haushaltsbehörde, dass in neu entstehenden Bereichen mit hoher Priorität, wie der Cybersicherheit, nach wie vor zu wenig Stellen zur Verfügung stehen, vor allem in den internen operativen Dienststellen.

Bei der Bezugnahme auf die Fortschritte in den Bereichen Governance und Risikomanagement sollte berücksichtigt werden, dass die Überwachung der Einhaltung der Vorschriften nun von der Pilotphase zur vollständigen Einführung übergeht. Daher ist es verständlich, dass der Abdeckungsgrad bisher recht gering ist. Dieses Projekt zur Einhaltung der Vorschriften ist die nächste Phase eines langfristigen Prozesses zur Verbesserung des Reifegrads im Bereich der Cybersicherheit, der mit der Festlegung einer gemeinsamen Methode für die Risikobewertung, der Entwicklung gemeinsamer Instrumente, der Einführung eines Schwachstellenmanagements und der Überwachung, Prüfung und Validierung des Anlagenbestands begann. Auf diesem langen Weg wurden trotz der Komplexität des Anlagenbestands der Kommission mit mehr als 1000 Informationssystemen, die von mehr als 50 Generaldirektionen und Exekutivagenturen betrieben werden, Fortschritte erzielt.

2. Kooperationsmechanismen der EU-OESS

Das CERT-EU ist dank seiner Mitwirkung als Vollmitglied in dem Netzwerk der Computer-Notfallteams (CSIRT-Netz), das im Rahmen der NIS-Richtlinie eingerichtet wurde, eine beeindruckende Erfolgsgeschichte bei der Förderung der Zusammenarbeit nicht nur zwischen den EU-OESS, sondern auch auf europäischer Ebene. So ist das CERT-EU ein Beispiel dafür, wie Zusammenarbeit und Cybersicherheitsdienste verbessert werden können. Die Bemerkungen des Rechnungshofes zum CERT-EU veranschaulichen sehr deutlich die hervorragende Arbeit, die das CERT-EU angesichts einer zunehmend feindseligen Bedrohungslage im Bereich der Cybersicherheit und einer chronisch unzureichenden Mittelausstattung leistet.

Im Rahmen der derzeitigen Interinstitutionellen Vereinbarung sind die dezentralen Agenturen und gemeinsamen Unternehmen der EU offiziell im Lenkungsausschuss des CERT-EU durch die ENISA vertreten. Darüber hinaus werden ihre Standpunkte in den Sitzungen des Lenkungsausschusses von einem Vertreter des Beratenden Ausschusses für Informations- und Kommunikationstechnologien (ICTAC) geäußert, der zwar an den Sitzungen teilnehmen darf, um die ENISA in ihrer Rolle als

Vertreter der Agenturen zu unterstützen, aber keinen formellen Sitz und keine formelle Stimme hat. Der Aspekt der angemessenen Vertretung der Agenturen im Lenkungsausschuss des CERT-EU wird in der vorgeschlagenen Verordnung behandelt, indem die Zusammensetzung des Lenkungsausschusses um bis zu drei Vertreter ergänzt wird, die vom Netz der EU-Agenturen (EUAN) auf Vorschlag seines ICTAC benannt werden.

Die Teilnahme an der Untergruppe „Cybersicherheit" des ICDT erfolgt nach bestem Bemühen auf dem von der jeweiligen EU-OESS festgelegten Beteiligungsgrad. Die Verbesserung des Informationsaustauschs bei der Beschaffung – ein wichtiges Thema im Rahmen der Taskforce 2 der Untergruppe „Cybersicherheit" – wird bei der Vorbereitung des neuen Rahmenvertrags für Cybersicherheit behandelt.

Hinsichtlich gemeinsamer Anwendungen für Dienste wie E-Mail und Videokonferenzen gibt es bereits die Möglichkeit, das von der Kommission für alle EU-OESS eingeführte SECEM-2-System für verschlüsselte E-Mails zu nutzen, das auf einer wirksamen Verwaltung von Verschlüsselungscodes und Zertifikaten beruht. Darüber hinaus wird derzeit SECABC entwickelt, eine Anwendung zur Verschlüsselung von E-Mails zwischen Einrichtungen, die ab 2022 allen interessierten EU-OESS zur Verfügung stehen soll. Sichere Videokonferenzen für nicht als Verschlusssache eingestufte sensible Informationen sind bereits möglich und können ad hoc auf andere EU-OESS ausgeweitet werden, indem die Identitäten der Sitzungsteilnehmer verwaltet werden. Der Austausch sensibler Informationen (z. B. durch gemeinsame Kennzeichnung und Handhabung) wird auch in der vorgeschlagenen Verordnung zur Informationssicherheit behandelt.

3. Austausch von Informationen über signifikante Sicherheitsvorfälle oder Schwachstellen

Der Tatsache, dass nicht alle EU-OESS bedeutende Vorfälle oder Schwachstellen dem CERT-EU melden, wird im Entwurf der Cybersicherheitsverordnung im Einklang mit dem Vorschlag der Kommission für die NIS-2-Richtlinie[1] Rechnung getragen. Der Grad der Umsetzung wird von den zusätzlichen Ressourcen abhängen, die die autonomen EU-OESS dafür bereitstellen. Der Spielraum für die Durchsetzung solcher Meldungen bleibt aufgrund der institutionellen Autonomie der EU-OESS begrenzt, auch im Rahmen der vorgeschlagenen Verordnung in der derzeit geplanten Form. Mit der vorgeschlagenen Verordnung über die Cybersicherheit werden Verfahren zur Einhaltung der Vorschriften geschaffen, die dem Ziel und dem Anwendungsbereich der neuen Vorschriften angemessen sind, ohne die Autonomie der EU-OESS zu beeinträchtigen.

[1] Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union und zur Aufhebung der Richtlinie (EU) 2016/1148 (COM(2020) 823 final).

III. ANTWORTEN DER KOMMISSION AUF DIE SCHLUSSFOLGERUNGEN UND EMPFEHLUNGEN DES EURH

Empfehlung 1 – Bessere Vorbereitung der EU-OESS auf Cyberbedrohungen durch gemeinsame verbindliche Vorschriften und die Aufstockung der Mittel für das CERT-EU

Der vorgeschlagene Verordnungstext wird spezifische Maßnahmen zur weiteren Erhöhung des gemeinsamen Cybersicherheitsniveaus enthalten. Diese Maßnahmen werden in Cybersicherheitspläne umgesetzt, die auf der Ebene der EU-OESS im Rahmen ihres eigenen Governance-Rahmens für Cybersicherheit festgelegt und umgesetzt werden.

Die Kommission akzeptiert diese Empfehlung. In Bezug auf die spezifischen Unterempfehlungen stellt die Kommission Folgendes fest:

a) Die Kommission akzeptiert die Empfehlung 1a. Der Entwurf der Verordnung wird Bestimmungen über Governance- und Kontrollrahmen enthalten, die auf der höchsten Führungsebene der einzelnen EU-OESS eingerichtet werden, um ein wirksames und umsichtiges Management aller Cybersicherheitsrisiken zu gewährleisten.
b) Die Kommission akzeptiert die Empfehlung 1b. Im Entwurf der Verordnung wird der Hinweis auf den risikobasierten Ansatz für das Cybersicherheitsmanagement untermauert, indem klargestellt wird, dass Maßnahmen, IT-Sicherheitspläne und die tatsächliche Durchführung wesentlicher Kontrollen auf die Bewertungen folgen sollten.
c) Die Kommission akzeptiert die Empfehlung 1c. Bildungs-, Sensibilisierungs- und Schulungsprogramme im Bereich der Cybersicherheit werden im Verordnungsentwurf als Teil der Grundlagen der Cybersicherheit genannt.
d) Die Kommission akzeptiert die Empfehlung 1d. Erfahrungsgemäß sind regelmäßige Prüfungen und Tests zwar wichtig, reichen aber nicht aus, um sicherzustellen, dass Fortschritte erzielt werden. Daher ist eine regelmäßige Berichterstattung und Transparenz als Teil des Governance-Rahmens für Cybersicherheit im Einklang mit Empfehlung 1a erforderlich.
e) Die Kommission akzeptiert die Empfehlung 1e. Im Verordnungsentwurf werden Bestimmungen über die Meldung bedeutender Cyberbedrohungen, -schwachstellen und -vorfälle an das CERT-EU durch die EU-OESS enthalten sein.
f) Die Kommission akzeptiert die Empfehlung 1f. Die Kommission schließt sich der Auffassung an, dass die Ressourcen des CERT-EU verstärkt werden müssen. Bestimmungen zur Personalausstattung und zu den Finanzbeiträgen der EU-OESS werden in den Text des Verordnungsentwurfs aufgenommen.
g) Die Kommission akzeptiert die Empfehlung 1g. In der vorgeschlagenen Verordnung werden Verfahren zur Einhaltung der Vorschriften vorgesehen, die dem Ziel und dem Anwendungsbereich der Bestimmungen angemessen und verhältnismäßig sind, wobei die institutionelle Autonomie der EU-OESS gewahrt bleibt. Der Inhalt der künftigen Verordnung hängt vom Ergebnis des Gesetzgebungsverfahrens ab und beruht auf einer Entscheidung der gesetzgebenden Organe der EU zum Vorschlag der Kommission.

Empfehlung 2 – Schaffung weiterer Synergien zwischen EU-OESS in ausgewählten Bereichen

Die Kommission, die derzeit den Vorsitz in der Untergruppe „Cybersicherheit“ des Interinstitutionellen Ausschusses für den digitalen Wandel (ICDT) innehat, stimmt den Empfehlungen zur Förderung von Lösungen für den kohärenten und sicheren Austausch sensibler Informationen, den systematischen Austausch von Informationen zu Cybersicherheitsprojekten und zur Festlegung des gemeinsamen Beschaffungsrahmens und der Verträge für Dienstleistungen im Bereich der Cybersicherheit zu.

Die Kommission akzeptiert diese Empfehlung. In Bezug auf die spezifischen Unterempfehlungen stellt die Kommission Folgendes fest:

a) Die Kommission akzeptiert die Empfehlung 2a. Die Kommission bringt technische Initiativen und Dienste in die Untergruppe „Cybersicherheit“ des ICDT ein, um gemeinsame Instrumente für den Austausch sensibler Informationen, die Dienste wie E-Mail und Videokonferenzen ermöglichen, zu fördern und zu unterstützen. Die Kommission stellt außerdem fest, dass gemeinsame Regeln für die Kennzeichnung und Handhabung von nicht als Verschlusssache eingestuften sensiblen Informationen in der vorgeschlagenen Verordnung über die Informationssicherheit behandelt werden.
b) Die Kommission akzeptiert die Empfehlung 2b. Die bestehenden Taskforces im Rahmen der Untergruppe „Cybersicherheit“ des ICDT befassen sich mit diesem Thema und werden es weiter vertiefen. Verbesserungen beim Informationsaustausch über die Beschaffung werden bei der Vorbereitung des neuen Rahmenvertrags für Cybersicherheit in Angriff genommen.
c) Die Kommission akzeptiert die Empfehlung 2c. Die EU-OESS haben bereits Zugang zu interinstitutionellen Rahmenverträgen im Bereich der IKT, die von der Kommission verwaltet werden. Die Ausarbeitung des neuen Rahmenvertrags für Cybersicherheit wird mit der Untergruppe „Cybersicherheit“ des ICDT koordiniert.

Empfehlung 3 – Verstärkte Schwerpunktsetzung des CERT-EU und der ENISA auf weniger gut gerüstete EU-OESS

Diese Empfehlung ist an das CERT-EU und die ENISA gerichtet.