



Rückmeldung des Vorsitzenden des Lenkungsausschusses des IT-Notfallteams für die Organe, Einrichtungen und sonstigen Stellen der EU (CERT-EU) und der Agentur der Europäischen Union für Cybersicherheit (ENISA) zu dem Sonderbericht des Europäischen Rechnungshofes zur Cybersicherheit bei den Organen, Einrichtungen und sonstigen Stellen der Union

1. Zusammenfassung

Angesichts der sich immer weiter verschärfenden Cyber-Bedrohungslage, ist das Thema Cybersicherheit von außerordentlicher Wichtigkeit und sehr kritisch für die Organe, Einrichtungen und sonstigen Stellen der Union, die in den letzten Jahren zunehmend Opfer technisch hoch entwickelter Cyberattacken wurden. Im Rahmen ihrer Aufträge, können die Agentur der Europäischen Union für Cybersicherheit (ENISA) und das IT-Notfallteam für die Organe, Einrichtungen und sonstigen Stellen der EU (CERT-EU) den Organen, Einrichtungen und sonstigen Stellen der EU (EUIBA) auf verschiedenen Ebenen wertvolle Unterstützung in puncto Cybersicherheit bieten. Der Vorschlag der Europäischen Kommission für eine Verordnung zu Maßnahmen für ein gemeinsames hohes Niveau der Cybersicherheit bei den Organen, Einrichtungen und sonstigen Stellen der EU, ist in diesem Zusammenhang ein Schlüsselinstrument, ein Instrument, das sowohl ENISA, CERT-EU als auch der Vorsitzende des Lenkungsausschusses des CERT-EU nachdrücklich unterstützen.

Zu diesem Zweck begrüßen ENISA, CERT-EU und der Vorsitzende des Lenkungsausschusses des CERT-EU den Sonderbericht des Europäischen Rechnungshofes zur Cybersicherheit bei den Organen, Einrichtungen und sonstigen Stellen der EU. Der Bericht kommt genau im richtigen Moment, um den aktuellen Stand der Vorbereitung der Organe, Einrichtungen und sonstigen Stellen der EU in ihrer Gesamtheit auf Cyberangriffe anzusprechen. Der Bericht hebt deutlich die zentrale Rolle hervor, die die Agentur der Europäischen Union für Cybersicherheit (ENISA) und das IT-Notfallteam für die Organe, Einrichtungen und sonstigen Stellen der EU (CERT-EU) im Hinblick auf dieses Thema spielen. Der Sonderbericht legt den Bedarf an weiteren Ressourcen und konkreten Maßnahmen dar, die direkt auf die Verbesserung der Cybersicherheitslage der Organe, Einrichtungen und sonstigen Stellen der EU ausgerichtet sind.



In diesem Sinne unterstützen ENISA, CERT-EU und der Vorsitzende des Lenkungsausschusses des CERT-EU die wichtigsten Feststellungen und Empfehlungen aus dem Sonderbericht, die auch auf die Gesetzesvorschläge der Europäischen Kommission in den Bereichen Cybersicherheit und Informationssicherheit bei den Organen, Einrichtungen und sonstigen Stellen der EU abgestimmt sind.

Die Kommentare im folgenden Abschnitt sollen einige Bereiche des Sonderberichts näher erläutern, insbesondere im Hinblick auf die einschlägigen Maßnahmen, die ENISA und/oder CERT-EU bereits ergriffen haben, und auf die geplanten Maßnahmen von ENISA und/oder CERT-EU, insbesondere im Bereich des Kapazitätsaufbaus für die Organe, Einrichtungen und sonstigen Stellen der EU. Was die Empfehlungen angeht, übernehmen ENISA und CERT-EU die Empfehlung 3 (Verstärkung der Konzentration von CERT-EU und ENISA auf weniger ausgereifte Organe, Einrichtungen und sonstige Stellen der EU), die sich gezielt an diese beiden Einrichtungen wendet.

2. Wesentliche Feststellungen

ENISA und CERT-EU unterstützen die vom Europäischen Rechnungshof gemachten Feststellungen. Allerdings werden unten stehend einige weitere Erläuterungen gegeben, insbesondere im Hinblick auf die bereits von ENISA und/oder CERT-EU umgesetzten Maßnahmen und die Pläne, die bereits für zukünftige Aktivitäten vorliegen.

Absatz 49

In Bezug auf die formale Anfrage, die der Beratungsausschuss für Informations- und Kommunikationstechnologie (ICTAC) an den Vorsitzenden des Lenkungsausschusses des CERT-EU zum Thema Stimmrecht im Verwaltungsrat gestellt hat, möchten wir Folgendes erläutern:

Angesichts des beträchtlichen Verwaltungsaufwands, den die Prüfung der aktuellen Interinstitutionellen Vereinbarung mit sich gebracht hätte, und da im Rahmen der laufenden Arbeiten an der „Verordnung über Maßnahmen für ein hohes gemeinsames Niveau an Cybersicherheit bei den Organen, Einrichtungen und sonstigen Stellen der EU“ bereits die Vertretung dezentraler Agenturen angesprochen wurde, wurde beschlossen, die Sache langfristig formal durch die Verordnung zu regeln. Bis dahin werden, wie der Vorsitzende



bestätigte, die aktuellen Praktiken fortgeführt und die Vertreter des ICTAC dürfen gern weiterhin ihre Ansichten vorbringen. Diese Ansichten werden der Fairness halber so weit wie möglich berücksichtigt.

Absatz 66

Ende 2021 hat die ENISA einen Aktionsplan für Cybersicherheitsübungen entwickelt, der ausdrücklich die Organe, Einrichtungen und sonstigen Stellen der EU mit einbezieht. Im 1. Quartal 2022 wird ein entsprechender Aktionsplan für Cybersicherheitsübungen bei den Organen, Einrichtungen und sonstigen Stellen der EU bereitgestellt.

BOX 3

Es wird zwar nicht ausdrücklich in den operativen Ergebnissen erwähnt, aber die ENISA hat verschiedene Organe, Einrichtungen und sonstige Stellen der EU unterstützt und mit diesen auf Grundlage der gestellten Anfragen zusammengearbeitet. So beispielsweise im Jahr 2018 unter dem Ziel 2.2. Unterstützung bei der Implementierung der EU-Politik:

- Die Europäische Zentralbank hat Unterstützung bei der Entwicklung der Eurosystem Red Team Test-Rahmenumgebung angefragt.
- Die Agentur der Europäischen Union für Flugsicherheit hat Unterstützung bei der Entwicklung der Ziele für das Europäische Zentrum für Cybersicherheit in der Luftfahrt, sowie bei der Sensibilisierung für Cybersicherheit und der sektoralen Umsetzung der Richtlinie zur Netz- und Informationssicherheit angefragt.
- Die Eisenbahnagentur der Europäischen Union hat Unterstützung bei der Umsetzung der NIS-Richtlinie im Bahnsektor angefragt, insbesondere bei der Entwicklung eines sektoralen Informationsaustausch- und Analysezentrums (ISAC) für Infrastrukturbetreiber und Eisenbahnunternehmen. Auch beim Kapazitätsaufbau (Organisieren von Schulungen und Trainings zur Sensibilisierung) war Unterstützung erwünscht.
- Die Agentur der Europäischen Union für Cybersicherheit hat die Agentur der Europäischen Union für das Betriebsmanagement von IT-Großsystemen im Raum der Freiheit, der Sicherheit und des Rechts (eu-LISA) bei deren Bemühungen um die Verbesserung der



Leistungsfähigkeit in den Bereichen Cybersicherheit und Geschäftskontinuität unterstützt. Die ENISA hat insbesondere ihr Fachwissen im Bereich der Organisation von Übungen und der Szenarienentwicklung bereitgestellt und der eu-LISA den vollständig entwickelten zivilen Notfallplan der ENISA zur Verfügung gestellt, um eine Notfallvorsorgeübung für eines der wichtigsten IT-Systeme der EU organisieren.

Außerdem arbeitet die ENISA seit 2019 aktiv mit den Organen, Einrichtungen und sonstigen Stellen der EU (z. B. ERA, EMSA, EASA, ACER) zusammen, um die Umsetzung der NIS-Richtlinie zum Aufbau des sektorspezifischen Aufbaus von Fachwissen und zur Sensibilisierung für Cybersicherheit sowie die damit in Zusammenhang stehenden sektoralen politischen Initiativen im Bereich Cybersicherheit zu unterstützen.

Absatz 71

Die ENISA hat 2021 ein Spezialtraining zum Thema „Aufbau eines Sensibilisierungsprogramms und Anwendung von Planübungen“ entwickelt, das 2022 freigegeben wird und sich gezielt an die Organe, Einrichtungen und sonstigen Stellen der EU wendet. Im Rahmen ihrer strukturierten Zusammenarbeit bieten ENISA und CERT-EU 2022 gemeinsame Weiterbildungen für die Organe, Einrichtungen und sonstigen Stellen der EU an.

Absatz 72

Es sollte beachtet werden, dass die Cybersicherheitsübungen der ENISA ein breites Spektrum abdecken und sich an eine breite Zielgruppe wenden, darunter auch an die Organe, Einrichtungen und sonstigen Stellen der EU. Dieser Ansatz entspricht auch den Bedürfnissen der Organe, Einrichtungen und sonstigen Stellen der EU, da diese von solchen Übungen mit den Vertretern von Mitgliedstaaten der EU deutlich profitieren können. An dieser Stelle sei erwähnt, dass die ENISA die technischen Bediensteten der Organe, Einrichtungen und sonstigen Stellen der EU seit 2016 als Handlungsträger in den Cyber Europe-Übungen einsetzt, unter Leitung des CERT-EU, dem engagierten Planer dieser Übungen. Als Fortsetzung dieser Bemühungen plant die ENISA in ihrer Übungsstrategie zu den Aktivitäten zum Kapazitätsaufbau 2022, eine neue Übung anzubieten, die mit Unterstützung des CERT-EU bereitgestellt wird und den Organen, Einrichtungen und sonstigen Stellen der EU eine Schulung in Form von Selbstbewertungsübungen ermöglicht.



3. Schlussfolgerungen und Empfehlungen

ENISA und CERT-EU übernehmen die Empfehlung 3 (Verstärkung der Konzentration von CERT-EU und ENISA auf weniger ausgereifte Organe, Einrichtungen und sonstige Stellen der EU), die sich gezielt an diese beiden Einrichtungen wendet.