EUROPÄISCHER RECHNUNGSHOF

DE

Pressemitteilung

Luxemburg, den 29. März 2022

EU-Institutionen müssen sich besser gegen Cyberangriffe wappnen

Die Einrichtungen der EU werden immer häufiger zum Ziel von Cyberangriffen. Ihre Cyberabwehr ist unterschiedlich stark entwickelt, insgesamt jedoch sind sie gegen die zunehmenden Bedrohungen nicht ausreichend gewappnet. Da die EU-Institutionen eng miteinander verflochten sind, können Schwachstellen bei einer von ihnen zu Sicherheitsbedrohungen auch für andere führen. Dies geht aus einem Sonderbericht des Europäischen Rechnungshofs zur Cybersicherheit in den Einrichtungen der EU hervor. Die Prüfer empfehlen die Einführung verbindlicher Vorschriften zur Cybersicherheit und eine Aufstockung der Ressourcen des IT-Notfallteams der EU (CERT-EU). Auch sollte sich die Europäische Kommission für eine stärkere Zusammenarbeit der EU-Institutionen einsetzen, und das CERT-EU sowie die EU-Agentur für Cybersicherheit sollten sich vordringlich denjenigen EU-Einrichtungen widmen, die bei der Cybersicherheit Nachholbedarf haben, so die Prüfer.

Zwischen 2018 und 2021 hat sich die Zahl der schweren Cybersicherheitsvorfälle in den EU-Einrichtungen mehr als verzehnfacht; durch die Zunahme der Arbeit aus dem Homeoffice haben Hacker nun eine deutlich größere potenzielle Angriffsfläche. Schwere Sicherheitsvorfälle werden in der Regel durch komplexe Cyberangriffe verursacht, bei denen meist neue Methoden und Technologien zum Einsatz kommen. Es kann dann Wochen oder sogar Monate dauern, einen solchen Vorfall zu untersuchen und die Schäden zu beheben. Ein Beispiel dafür ist der Cyberangriff auf die Europäische Arzneimittelagentur, bei dem sensible Daten geleakt und manipuliert wurden, um das Vertrauen in Impfstoffe zu untergraben.

"*Die Organe, Einrichtungen und sonstigen Stellen der EU sind attraktive Ziele für potenzielle Angreifer und insbesondere für Gruppen, die in der Lage sind, technisch anspruchsvolle verdeckte Angriffe zum Zweck der Cyberspionage und anderen schädlichen Zwecken durchzuführen*", so Bettina Jakobsen, das für die Prüfung zuständige Mitglied des Europäischen Rechnungshofs. "*Solche Angriffe können weitreichende politische Folgen haben, dem Ruf der EU insgesamt schaden und das Vertrauen in ihre Organe untergraben. Die EU muss mehr dafür tun, ihre eigenen Behörden zu schützen.*"

Die wichtigste Feststellung der Prüfer war, dass die Organe, Einrichtungen und sonstigen Stellen der EU nicht immer ausreichend gegen Cyberbedrohungen geschützt sind. Die EU-Institutionen verfolgten bei der Cybersicherheit keinen einheitlichen Ansatz, bisweilen fehle es an

Diese Pressemitteilung enthält die Hauptaussagen des Sonderberichts des Europäischen Rechnungshofs. Bericht im Volltext unter www.eca.europa.eu.

ECA Press

12, rue Alcide De Gasperi – L-1615 Luxembourg

E: press@eca.europa.eu @EUAuditors eca.europa.eu

grundlegenden Kontrollen und bewährten Verfahren für den Umgang mit Cyberbedrohungen und das Personal werde nicht systematisch in Cybersicherheitsfragen geschult, so die Prüfer. Außerdem werde unterschiedlich stark in die Cybersicherheit investiert – auch bei von der Größe her vergleichbaren EU-Einrichtungen seien die Abweichungen erheblich. Unterschiede beim Schutz vor Cyberangriffen könnten zwar theoretisch durch das unterschiedliche Risikoprofil der einzelnen Behörden und die unterschiedlich hohe Sensibilität der von ihnen verarbeiteten Daten begründet werden. Dennoch könnten Schwachstellen in einer einzigen EU-Einrichtung die Cybersicherheit in mehreren anderen Einrichtungen bedrohen, da die EU-Einrichtungen alle untereinander und oft auch mit öffentlichen und privaten Organisationen in den Mitgliedstaaten vernetzt sind.

Das IT-Notfallteam (CERT-EU) und die Agentur der Europäischen Union für Cybersicherheit (ENISA) sind die beiden wichtigsten Stellen der EU für die Hilfestellung bei Cybersichersicherheitsfragen. Sie hätten jedoch wegen knapper Ressourcen oder anderer Prioritäten den EU-Einrichtungen nicht die nötige Unterstützung bieten können. Auch beim Informationsaustausch gibt es den Prüfern zufolge Probleme. So meldeten nicht alle EU-Einrichtungen umgehend ihre Erkenntnisse über Sicherheitslücken und schwere Cybervorfälle, von denen sie betroffen sind und die sich auch auf andere auswirken könnten.

Hintergrundinformationen

Derzeit gibt es keinen Rechtsrahmen für die Informations- und Cybersicherheit in den Organen, Einrichtungen und sonstigen Stellen der EU. Für diese gilt nämlich weder die sogenannte NIS-Richtlinie aus dem Jahr 2016, bei der es sich um die umfassendste Rechtsvorschrift der EU zur Cybersicherheit handelt, noch deren Vorlage für eine überarbeitete Fassung, die NIS-2-Richtlinie. Es liegen auch keine vollständigen Informationen darüber vor, wie viel Geld die EU-Einrichtungen für Cybersicherheit ausgeben. Die im Juli 2020 veröffentlichte Mitteilung der Europäischen Kommission über die EU-Strategie für eine Sicherheitsunion für den Zeitraum 2020-2025 enthält gemeinsame Vorschriften zur Informations- und Cybersicherheit für alle EU-Einrichtungen. In der Cybersicherheitsstrategie der EU für die "digitale Dekade", die im Dezember 2020 veröffentlicht wurde, verpflichtete sich die Europäische Kommission, einen Vorschlag für eine Verordnung über gemeinsame Cybersicherheitsvorschriften für alle EU-Einrichtungen vorzulegen. Außerdem schlug sie vor, eine neue Rechtsgrundlage für das CERT-EU zu schaffen, um dessen Mandat zu stärken und es mit mehr Mitteln auszustatten.

Der Sonderbericht 05/2022 "*Cybersicherheit: Organe, Einrichtungen und sonstige Stellen der EU sind insgesamt nicht ausreichend gegen Bedrohungen gewappnet*" ist auf der Website des Europäischen Rechnungshofs abrufbar. Der Europäische Rechnungshof wies bereits 2019 in einer Analyse auf die Herausforderungen für eine wirksame Cybersicherheitspolitik der EU hin.

Pressekontakt

Pressestelle des Hofes: press@eca.europa.eu

- Claudia Spiti: claudia.spiti@eca.europa.eu – Mobil: (+352) 691 553 547
- Vincent Bourgeais: vincent.bourgeais@eca.europa.eu – Mobil: (+352) 691 551 502
- Damijan Fišer: damijan.fiser@eca.europa.eu – Mobil: (+352) 621 552 224