Stellungnahme

Gewerkschaft der Polizei
Bundesvorstand

Stellungnahme der Gewerkschaft der Polizei (GdP)

zum Referentenentwurf des
Bundesministeriums des Innern

Entwurf eines Gesetzes zur Durchführung der Verordnung (EU) 2024/2847 über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen (Cyberresilienz-Verordnung)

Berlin, 01.04.2026
Abt. Innenpolitik | AL3

Die Gewerkschaft der Polizei (GdP) - mit über 210.000 Mitgliedern größte Polizeigewerkschaft hierzulande - nimmt zum vorliegenden Referentenentwurf des BMI; Entwurf des Durchführungsgesetzes zur EU-Verordnung über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen (Cyber Resilience Act – CRA) wie folgt Stellung:

I. - Bewertung der polizeilichen Effizienzgewinne

Wir begrüßen die Zielsetzung des Gesetzentwurfs, die Cybersicherheit vernetzter Produkte über deren gesamten Lebenszyklus hinweg zu stärken. Aus polizeilicher Sicht ergeben sich daraus signifikante Optimierungspotenziale für die operative Arbeit:

- **Präventionswirkung durch Standardisierung:** Die gesetzliche Verpflichtung der Hersteller zu **„Security by Design“** und **„Security by Default“** adressiert die Ursachen zahlreicher Cyber-Straftaten bereits auf der Produktebene. Eine Reduktion systemimmanenter Schwachstellen führt perspektivisch zu einer Entlastung der Ermittlungsbehörden bei der Bearbeitung von Massenphänomenen im Bereich der Computerkriminalität.

- **Optimierung der IT-Forensik:** Die im CRA vorgesehenen Dokumentationspflichten und die Transparenz über die technische Architektur von Produkten erleichtern die **digitale Spurensicherung**. IT-forensische Untersuchungen können zielgerichteter durchgeführt werden, da die Identifikation und Analyse von Schwachstellen sowie die Rekonstruktion von Angriffsvektoren durch standardisierte Herstellerangaben unterstützt werden.

- **Effektives Schwachstellenmanagement:** Die verpflichtende Meldung und zeitnahe Behebung aktiv ausgenutzter Schwachstellen verbessert die Informationslage der Sicherheitsbehörden und ermöglicht eine schnellere Reaktion auf neue Bedrohungslagen.

II. - Analyse der Implementierungsrisiken

Trotz der positiven Zielsetzung identifiziert die GdP kritische Faktoren für die praktische Umsetzung:

- **Administrativer Mehraufwand und Ressourcenbindung:** Die Überwachung der Einhaltung sowie die Verarbeitung der eingehenden Meldungen erfordern erhebliche personelle und technische Kapazitäten in den zuständigen Behörden. Ohne eine entsprechende Ressourcenausstattung droht eine Überlastung der fachspezifischen Abteilungen, was die intendierte Sicherheitswirkung mindern könnte.

- **Herausforderungen im Vollzug:** Die Durchsetzung der Anforderungen gegenüber Herstellern außerhalb des europäischen Rechtsraums stellt eine erhebliche Hürde dar. Ein Vollzugsdefizit in diesem Bereich könnte zu Wettbewerbsnachteilen für europäische Unternehmen führen, ohne die Cybersicherheit in der Breite nachhaltig zu erhöhen.

- **Komplexität der Meldewege:** Eine zu bürokratische Ausgestaltung der Meldepflichten könnte den Informationsfluss verzögern. Für die polizeiliche Gefahrenabwehr und Strafverfolgung ist jedoch ein unmittelbarer Zugriff auf sicherheitsrelevante Informationen essenziell.

III. - Abschließende Abwägung und Fazit

In der Gesamtabwägung zwischen den identifizierten Risiken und den zu erwartenden Synergieeffekten **befürwortet** die GdP das vorliegende Durchführungsgesetz.

Die **strukturelle Verbesserung der digitalen Sicherheitsarchitektur** durch verbindliche Herstellerpflichten ist eine notwendige Voraussetzung für eine zukunftsfähige Polizeiarbeit im digitalen Raum.

Um den Erfolg des Gesetzes zu gewährleisten, fordert die GdP jedoch eine **praxisnahe Ausgestaltung der Meldeverfahren** sowie eine begleitende Aufstockung der personellen und technischen Ressourcen in den IT-Fachbereichen der Polizei und der Aufsichtsbehörden.