Stellungnahme

Gewerkschaft der Polizei
Bundesvorstand

Stellungnahme der Gewerkschaft der Polizei (GdP)

zum Referentenentwurf des Bundesministeriums des Innern über ein

Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung

Berlin, 01.07.2025
mf

Zusammenfassung

- keine Einschränkung der Handlungsfähigkeit des öffentlichen Dienstes durch steigende Abhängigkeit von digitalen Technologieanbietern erlauben
- EU-weite, einheitliche Standards sind erforderlich
- bundesweit einheitliche Standards zur Abwehr von Cyber-Attacken sind vonnöten
- GdP begrüßt die vorgesehenen Sanktionierungsmöglichkeiten bei Nichteinhaltung/-umsetzung der Vorgaben
- Anbieter von Softwarelösungen sollten in Haftung genommen werden, sofern sie bekannte Sicherheitslücken in ihren Produkten nicht schließen und dadurch Schäden entstehen
- Sicherheitsbehörden müssen mit der Zeit gehen
- Digitalisierung der Sicherheitsbehörden sollte höchste Priorität erhalten
- GdP hält die Einrichtung eines Digitalisierungsfonds für sinnvoll
- Datenübermittlungsmöglichkeiten des BSI an die Polizeien werden seitens der GdP begrüßt
- Vorhaben hätte noch stärkeren Fokus auf polizeiliche Belange legen müssen
- Vorhaben darf nicht nur zu noch mehr Compliance-Vorschriften ohne gleichzeitige Erhöhung des IT-Sicherheitsniveaus führen
- Bei grenzüberschreitenden polizeilichen Ermittlungen wegen Cybercrime-Delikten musss weiterhin das Bundeskriminalamt (BKA) federführend bleiben. Hier darf dem BSI nur eine beratend-unterstützende Rolle zukommen.
- Das BKA muss die gesetzliche Kompetenz zur Abwehr schwerwiegender Cyber-Angriffe erhalten.

Vorbemerkung

Mit über 209.000 Mitgliedern ist die GdP die größte Polizeigewerkschaft in Deutschland und wir bedanken uns für die Möglichkeit, zum „Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung“ Stellung nehmen zu dürfen.

Stellungnahme

Aus Sicht der Gewerkschaft der Polizei (GdP) darf eine steigende Abhängigkeit von digitalen Technologieanbietern nicht zu Einschränkungen der Handlungsfähigkeit des öffentlichen Dienstes führen. Die Bundesregierung muss ernsthafte Schritte unternehmen, die digitale Souveränität sicherzustellen. Von Bedeutung ist die Umsetzung der NIS-2-Richtlinie in nationales Recht, da trotz unterschiedlicher Strukturen und Zuständigkeiten der Sicherheitsbehörden in der Europäischen Union entsprechende, einheitliche Standards gewährleistet sein müssen.

Insbesondere innerhalb der Bundesrepublik Deutschland müssen aufgrund der föderalen Strukturen bundesweit gültige Standards zur Abwehr und zum Schutz vor Cyberangriffen durch alle Akteure des öffentlichen Sektors eingeführt sowie eingehalten werden. Die vorgesehenen Sanktionierungsmöglichkeiten bei Nichteinhaltung/-umsetzung werden von der Gewerkschaft der Polizei (GdP) befürwortet. Der Ansatz des Computer Security Incident Response Teams (CSIRTs) wird in den Polizeien grundsätzlich verfolgt. Allerdings fehlen hierfür oftmals schlichtweg Fachkräfte aus dem IT-Sektor.

Angesichts der zunehmenden Digitalisierung des persönlichen wie gesellschaftlichen Lebens muss die Polizei aus unserer Sicht endlich in das 21. Jahrhundert geführt werden. Kriminelle verlagern ihre Aktivitäten schon seit längerem in den virtuellen Bereich. Sie profitieren einerseits von mangelnden digitalen Kompetenzen oder fehlendem Risikobewusstsein in der Bevölkerung oder in Unternehmen. Andererseits wissen sie, dass sie den Ermittlerinnen und Ermittlern – häufig auch technologisch – mehr als einen Schritt voraus sind. Es kann daher nicht überraschen, dass sich die Fallzahlen zur Internetkriminalität anhand der Polizeilichen Kriminalstatistik (PKS) für das Jahr 2024 sowie des Lagebildes Cybercrime des Bundeskriminalamtes (BKA) weiterhin auf hohem Niveau befinden.

Festzustellen ist zudem, dass immer mehr Cybercrime-Delikte aus dem Ausland heraus begangen werden, zumeist Erpressungen mit „Ransomware“. Viele Taten bleiben dabei im sogenannten Dunkelfeld. Der niedrigschwellige Zugang zu KI wird die Deliktzahlen noch einmal deutlich steigern.

Die Digitalisierung der Sicherheitsbehörden sollte höchste Priorität erhalten. Außerdem erwartet die Gewerkschaft der Polizei (GdP) ein höheres Tempo beim groß angelegten polizeilichen Digitalprojekt P20. Sinnvoll wäre aus unserer Sicht die Einrichtung eines Digitalisierungsfonds, der vor allem dem Bundeskriminalamt mit seiner Zentralstellenfunktion unter dem Motto „crimefighting as a service“ zugutekommen sollte. Natürlich sollten auch die Bundesländer auf

technischer Augenhöhe mitgenommen werden. Dafür müssen sich die Konferenz der Innenminister und -senatoren (IMK) sowie der Bundesinnenminister gegenüber den haushaltspolitisch Verantwortlichen stark machen.

Begrüßenswert aus Sicht der Gewerkschaft der Polizei (GdP) ist die im Referentenentwurf in Paragraf 3 Absatz 1 Nummer 18 Buchstabe a) des Gesetzes über das Bundesamt für Sicherheit in der Information-technik und über die Sicherheit in der Informationstechnik von Einrichtungen enthaltene Verpflichtung für das Bundesamt für Sicherheit in der Informationstechnik (BSI) die Polizeien des Bundes bei der Wahrnehmung ihrer gesetzlichen Aufgaben zu unterstützen.

Ebenfalls positiv bewertet die GdP die in Paragraf 8 Absatz 6 Nummer 1 des o.g. Gesetzes vorgesehene Möglichkeit des BSI, zur Abwehr einer Gefahr für die öffentliche Sicherheit, die unmittelbar von einem Schadprogramm ausgeht, auch personenbezogene Daten an die Polizeien von Bund und Ländern zu übermitteln. Dies ist für die polizeiliche Ermittlungstätigkeit sehr hilfreich.

Gleiches gilt für die in Paragraf 8 Absatz 7 Nummer 2 des genannten Gesetzes vorgesehene Datenübermittlungsmöglichkeit „an die Polizeien des Bundes und der Länder zur Abwehr einer Gefahr für den Bestand oder die Sicherheit des Staates oder Leib, Leben oder Freiheit einer Person oder Sachen von bedeutendem Wert, deren Erhalt im öffentlichen Interesse geboten ist“.

Für begrüßenswert hält die Gewerkschaft der Polizei (GdP) darüber hinaus die explizite Erwähnung der Polizeien des Bundes und der Länder als sogenannte „berechtigte Zugangsnachfrager“ gemäß Paragraf 2 Nummer 2 Buchstabe d) des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik und über die Sicherheit in der Informationstechnik von Einrichtungen.

Die Gewerkschaft der Polizei (GdP) regt jedoch textliche Änderungen mit Blick auf den sogenannten „Stand der Technik“ an. Hier sollte es nicht heißen, dass der Stand der Technik „nur“ eingehalten werden sollte. Vielmehr sollte es heißen, dass der Stand der Technik eingehalten werden müsse. Dies gilt unter anderem für die entsprechenden Bestimmungen in Paragraf 30 Absatz 2 und Paragraf 31 Absatz 2 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik und über die Sicherheit in der Informationstechnik von Einrichtungen.

Außerdem hätte sich die Gewerkschaft der Polizei (GdP) grundsätzlich eine noch stärkere Berücksichtigung polizeilicher Belange im Referentenentwurf gewünscht. Denn: Eine effektive Cybersicherheitsstrategie ist mit Blick auf die fortschreitende Digitalisierung, national wie international, einer der entscheidenden Schlüssel für die Gewährleistung der Inneren Sicherheit in Deutschland. Schließlich steigt die Zahl der von staatlichen oder nichtstaatlichen Akteuren begangenen Cyberangriffen seit Jahren an. Insbesondere Strukturen der Organisierten Kriminalität agieren professionell und gezielt im virtuellen Raum. Diese profitieren von noch unzureichenden Cyberabwehrstrukturen. Hier fehlt es an bundesweit gültigen Schutzstandards.

Des Weiteren plädiert die Gewerkschaft der Polizei (GdP) dafür, Hersteller von Softwarelösungen in Haftung zu nehmen, sofern diese bekannte Sicherheitslücken in ihren Produkten nicht schließen und dadurch Schäden verursacht werden.

Aus unserer Sicht darf die neue Gesetzgebung nicht nur zu einem Mehr an zu erfüllenden Compliance-Vorschriften führen, sondern muss auch zu einer tatsächlich messbaren Erhöhung der IT-Sicherheit beitragen. Bei länderübergreifenden Ermittlungen muss auch weiterhin dem Bundeskriminalamt (BKA) die Federführung obliegen. Dem BSI darf hier nur eine beratende Funktion zukommen.

Ziel des Gesetzesvorhabens sollte es nach Auffassung der Gewerkschaft der Polizei (GdP) sein, Cybercrime auch tatsächlich aktiv zu verhindern – sowohl für die Bürgerinnen und Bürger als auch für kleine und mittelständische Unternehmen, um diese noch besser bei der Aufrechterhaltung ihrer IT-Sicherheit und der eigenen digitalen Souveränität zu unterstützen.

Hierfür braucht es aus Sicht der Gewerkschaft der Polizei (GdP) auch mehr Befugnisse für das BKA im Kampf gegen Cyberkriminalität. Die Bedrohungslage aus dem virtuellen Raum ist vielfältig und nimmt zu. Gleichwohl verfügt das BKA momentan nur über die gesetzliche Zuständigkeit für die Strafverfolgung von Cybercrime. Die Behörde benötigt jedoch zudem dringend auch die Kompetenz zur Abwehr schwerwiegender Cyberangriffe.

Aktuell existiert die paradoxe Situation, dass das BKA in bestimmten Fällen zwar Cyberstraftaten nach einem Schadenseintritt verfolgen, Tatbegehung und potenziellen Schadenseintritt aber nicht durch Maßnahmen der konkreten Gefahrenabwehr im Vorfeld verhindern kann. Das macht eine ganzheitliche Bekämpfung schwerer Cyberkriminalität derzeit unmöglich.

Im Sinne einer effizienten Sicherheitspolitik müssen die Strafverfolgung und die polizeiliche Gefahrenabwehr in Zukunft aus Sicht der Gewerkschaft der Polizei (GdP) zentral und aus einer Hand erfolgen. Das BKA verfügt auch bereits über die Kompetenzen, die erforderliche Technik sowie über die nationalen und internationalen Netzwerke, um diese Aufgabe zu übernehmen.