Deutscher Bundestag **Drucksache 19/13739**

19. Wahlperiode 04.10.2019

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Andrej Hunko, Christine Buchholz, Dr. André Hahn, weiterer Abgeordneter und der Fraktion DIE LINKE.
– Drucksache 19/13291 –

EU-Krisenreaktionsprotokoll für grenzüberschreitende Cyberangriffe

Vorbemerkung der Fragesteller

Die Polizeiagentur Europol hat ein Krisenreaktionsprotokoll für grenzüberschreitende Cyberangriffe entwickelt („Law enforcement agencies across the EU prepare for major crossborder cyber attacks“, Europol vom 18. März 2019). Dieses „EU Law Enforcement Emergency Response Protocol“ (LE ERP) ist Teil des EU-Konzepts für die „koordinierte Reaktion auf grenzüberschreitende Cybersicherheitsvorfälle und -krisen in großem Maßstab“ von 2017 und soll die Strafverfolgungsbehörden in der Europäischen Union unterstützen. Zuständig ist hierfür das Europäische Zentrum für Cyberkriminalität (EC3) bei Europol. Dabei soll auf Cybersicherheitsereignisse reagiert werden, die sowohl von nationalen Akteuren als auch von „Cyberkriminellen“ gestartet wurden. Nur Vorfälle, die durch Naturkatastrophen, menschliches Versagen oder Systemversagen verursacht werden, fallen nicht in den Anwendungsbereich des Protokolls.

Das Krisenreaktionsprotokoll soll eine schnelle Bewertung des Vorfalls und den sicheren und zeitnahen Austausch kritischer Informationen gewährleisten. Hierzu gehören die Bereiche „Früherkennung und Identifizierung eines größeren Cyberangriffs; Einstufung der Bedrohung; Einrichtung eines Koordinierungszentrums für Notfallmaßnahmen; Frühwarnmeldungen; ein operationeller Aktionsplan für die Strafverfolgung; Untersuchung des Vorfalls; Schließen des Notfallprotokolls“.

1. Welche Details kennt die Bundesregierung zum „EU Law Enforcement Emergency Response Protocol“ für „erhebliche grenzüberschreitende Cyberangriffe“, und wie ist sie daran beteiligt?

Die Estnische Ratspräsidentschaft veranstaltete im September 2017 unter Beteiligung von 18 Mitgliedstaaten (MS) einen Workshop zur Thematik.

Dabei wurde das Erfordernis einer engen Zusammenarbeit bei erheblichen grenzüberschreitenden Cyberangriffen festgestellt. Europol solle dabei hinsichtlich der strafrechtlichen Verfolgung die zentrale koordinierende Rolle übernehmen. Darüber hinaus wurde der Bedarf an einem verbindlichen siche-

---

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern, für Bau und Heimat vom 2. Oktober 2019 übermittelt.

Die Drucksache enthält – in kleinerer Schrifttype – den Fragetext.

ren Kommunikationskanal sowie einer 24/7-Kommunikation von Regierungs-CERTs (Computer Emergency Response Teams) und Strafverfolgungsbehörden festgestellt. Im Rahmen der Sitzung des Ständigen Ausschuss für die operative Zusammenarbeit im Bereich der inneren Sicherheit (COSI) am 21. November 2017 fand der Vorschlag, ein „Emergency Response Protocol“ für koordinierte Reaktionen bei grenzüberschreitenden Cyberangriffen zu erstellen, breite Unterstützung.

Europol erarbeitete im Nachgang hierzu das EU Law Enforcement Emergency Response Protocol (i.F. LE ERP) für koordinierte Reaktionen bei grenzüberschreitenden schweren Cyberangriffen. Um eine gemeinsame Reaktion zu ermöglichen, sollen Sicherheitsvorfälle mit einem schwerwiegenden kriminellen Hintergrund gemeldet werden und bei Europol (ergänzend zu den jeweiligen betroffenen MS) entsprechend eines definierten Prozesses im Rahmen des Europol-Mandats bearbeitet werden. Die Umsetzung des Konzepts soll im Rahmen des EU-Politikzyklus 2018-2021 in der Priorität „Attacks against information systems“ erfolgen.

Nach Maßgabe von § 3 BKAG fungiert das BKA als nationale Stelle für EUROPOL nach § 1 des EUROPOL-Gesetzes. Als nationale Stelle für EUROPOL fungiert das BKA auch als 24/7 Law Enforcement National Point of Contact (i.F. NPoC) im Kontext des LE ERP.

2. Welche Konsequenzen ergeben sich durch das LE ERP für Bundesbehörden, und wie werden diese umgesetzt?

Das BKA unterstützt die mit dem LE ERP formulierte Zielsetzung durch die organisatorische Anbindung des LE ERP NPoC beim Phänomenbereich Cybercrime in der Abteilung Organisierte und Schwere Kriminalität (SO). Die mit dem LE ERP formulierten Kommunikationsanlässe umfassen dabei den für den internationalen polizeilichen Informationsaustausch mit EUROPOL definierten Rahmen. Eine von EUROPOL hierzu vorgehaltene Liste von 24/7 Erreichbarkeiten der an dem LE ERP teilnehmenden Staaten stellt dabei sicher, dass der für das Protokoll relevante Informationsaustausch bei zeitkritischen Vorfällen jederzeit erfolgen kann.

3. Welche Bundesbehörden sind dabei für welche Routinen des LE ERP zuständig (siehe Vorbemerkung der Fragesteller)?

Das BKA ist definierter NPoC und somit für alle mit dem LE ERP definierten Kommunikationsanlässe für Deutschland der designierte Ansprechpartner.

4. Mithilfe welcher vorhandenen technischen Verfahren soll das LE ERP die schnelle Bewertung eines Vorfalls gewährleisten, und welche weiteren Fähigkeiten sollen hierzu aufgebaut werden?

Die Identifizierung, Bewertung und Klassifizierung länderübergreifender Cybercrime-Vorfälle erfolgen bei EUROPOL auf Grundlage einer für diesen Bedarf entwickelten Bedrohungsmatrix (sog. Threat Matrix). Der Austausch der dafür erforderlichen Informationen erfolgt grundsätzlich durch den designierten NPoC über die zwischen EUROPOL und BKA bestehenden Informationskanäle. Sofern im Einzelfall erforderlich, bietet EUROPOL darüber hinaus den LE ERP-Teilnehmern optional sogenannte Virtual Command Posts (VCP) an. VCP bietet funktional verschlüsseltes Audio-/Video-Streaming sowie Kommunikation über einen Messenger-Dienst.

5. Inwiefern kann hierzu nach Maßgabe der Europol-Verordnung auch auf militärische Erkenntnisse zurückgegriffen werden, etwa aus den Mitgliedstaaten oder der NATO?

Die Europol-Verordnung enthält keine Regelungen, die ihrem Wortlaut nach Rückgriffe auf militärische Erkenntnisse betreffen, steht einem derartigen Vorgehen jedoch auch nicht entgegen, wenn und soweit dies der Erfüllung der Aufgaben von Europol nach Maßgabe der Europol-Verordnung dient.

6. Welche Details kennt die Bundesregierung zu den geplanten „operationellen Aktionsplänen für die Strafverfolgung“ nach einem Cyberangriff?

Der im LE ERP beschriebene „Law Enforcement Emergency Operational Action Plan“ (i.F. EOAP) bildet eine Stufe im Ablaufprozess des LE ERP ab. Der EOAP wird von EUROPOL dann ausgerufen, wenn eine staatenübergreifende Abstimmung, ggf. unter Hinzuziehung weiterer Akteure (z. B. Unternehmen), auf Grundlage der erfolgten Bewertung gemäß dem im Protokoll vorgesehenen Ablauf erforderlich erscheint.

7. Was ist der Bundesregierung über eine anstehende oder jüngst stattgefundene Cyberübung bei Europol bekannt, mit der auch Fähigkeiten zur „Abschreckung“ entwickelt werden sollen – Ratsdokument 10991/19 – (bitte das Datum, den Ort und die Teilnehmenden mitteilen)?

Das European Cybercrime Centre bei EUROPOL (EC3) veranstaltet am 31. Oktober 2019 eine eintägige Cyber-Simulationsübung (table top exercise). Gegenstand der Übung ist ein von EC3 gemeinsam mit der ENISA entwickeltes Cyberangriffsübungsszenario. Übungsziel ist es, das LE ERP auf Praxistauglichkeit zu testen. Eingebunden in die Übung sind neben den verantwortlichen Organisatoren Frankreich, EC3 und ENISA die CERT-EU, die European Defence Agency (EDA), Eurojust, die Niederlande, Spanien, Norwegen und der Privatsektor (Palo Alto sowie Citibank und Santander) aus den EUROPOL Advisory Groups (Internet Security und Financial Services).

8. Welche weiteren Übungen sollen nach Kenntnis der Bundesregierung im Rahmen des LE ERP durchgeführt werden, wann, und wo finden diese statt, und wer nimmt daran teil?

Die Bundesregierung verweist auf die Antwort zu Frage 7. Darüberhinausgehende Bestrebungen EUROPOLS zu Übungen im LE ERP Kontext sind hier nicht bekannt.

9. Welche gemeinsamen Ermittlungsgruppen sind nach Kenntnis der Bundesregierung im Rahmen des LE ERP geplant?

Sogenannte gemeinsame Ermittlungsgruppen (Joint Investigation Teams oder JITs) im Kontext des LE ERP bilden die Möglichkeit ab, auf konkrete Szenarien von Seiten der Strafverfolgung zur Durchführung strafrechtlicher Ermittlungen koordiniert zu reagieren. Absprachen hierzu erfolgen im konkreten Einzelfall anlassbezogen und lageabhängig nach Maßgabe des geltenden Rechts.

10. Welche gemeinsamen Aktionstage (auch „Cyber patrol actions weeks“) plant Europol zu kriminellen Cyberaktivitäten, und wann sollen diese stattfinden?

Nach Kenntnis der Bundesregierung plant Europol im Frühjahr 2020 einen „action month“. Im Fokus stehen hierbei Ermittlungen zu Nutzern, die auf bereits sichergestellten Darknet-Plattformen aktiv waren

a) Welche weiteren Partner, etwa Drittstaaten, Interpol, regionale Initiativen, Expertennetzwerke oder Firmen und Institute nehmen an den Maßnahmen teil?

Nach Kenntnis der Bundesregierung handelt es sich hierbei um eine Veranstaltung, die ausschließlich an Strafverfolgungsbehörden gerichtet ist. Hierbei ist grundsätzlich auch eine Teilnahme von Drittstaaten möglich, die ein operatives Abkommen mit Europol geschlossen haben.

b) Welche anderen Aktionstage bzw. Kriminalitätsphänomene werden in das mehrtägige „Cyber patrolling“ eingebunden (etwa Begünstigung irregulärer Einwanderung, Menschenhandel, Drogenhandel), um deren IT-Infrastruktur aufzudecken und zu bekämpfen?

Die Deliktsbereiche orientieren sich am Europol-Mandat entsprechend der Europol-Verordnung. Einzelheiten sind der Bundesregierung aktuell nicht bekannt.

11. Was ist der Bundesregierung über Inhalte und Ergebnisse diesjähriger Trainings zu „Cyber patrolling“ im Rahmen der Europäischen multidisziplinären Plattform gegen kriminelle Bedrohungen (EMPACT) bekannt?

Zu den Inhalten und Ergebnissen des diesjährigen Trainings zu „Cyber patrolling“ im Rahmen von EMPACT liegen der Bundesregierung zurzeit keine Kenntnisse vor. Der COSI berichtet hierzu voraussichtlich im Frühjahr 2020.

12. An welchen derartigen Trainings haben welche Bundesbehörden teilgenommen?

An derartigen Trainings haben bislang keine Bundesbehörden teilgenommen.

13. Was ist der Bundesregierung über Zwischenergebnisse einer Analyse zum Ausbau von Fähigkeiten des ATLAS-Verbunds europäischer Polizei-Spezialeinheiten bekannt, die nach Einrichtung eines Büros bei Europol (vgl. Bundestagsdrucksache 19/8193) unter anderem die Beschaffung und gemeinsame Nutzung von spezieller Ausrüstung, die Einrichtung gemeinsamer Truppenübungsplätze sowie den Aufwuchs zu einem „Exzellenzzentrum“ vorbereiten soll (Ratsdokument 10991/19), und wie hat sich die Bundesregierung hierzu in Debatten der zuständigen Ratsarbeitsgruppe positioniert?

Die Eröffnung des „ATLAS Unterstützungsbüros“ ist für Januar 2020 vorgesehen.

Hinsichtlich der Beschaffung und gemeinsamen Nutzung von Führungs- und Einsatzmittel der ATLAS-Spezialeinheiten bestehen nach Kenntnis der Bundesregierung derzeit keine konkreten Planungen.

In Bezug auf Trainingseinrichtungen in der Funktion als Exzellenzzentren sind für die Haushaltsjahre 2020/2021 der Ausbau einer bereits bestehenden Trainingsanlage in Italien zur Vorbereitung der ATLAS-Spezialeinheiten auf Einsätze zur Bewältigung von Flugzeugentführungen sowie die Etablierung eines Trainingszentrums für operative Einsatzmedizin in Ungarn zur Vorbereitung der ATLAS-Spezialeinheiten auf medizinische Ersthilfe für schwerstverletzte Personen vorgesehen.

Die Bundesregierung beteiligt sich an den Diskussionen über eine Weiterentwicklung der europäischen polizeilichen Zusammenarbeit, einschließlich des ATLAS-Netzwerkes. Auf die Antwort der Bundesregierung auf die Schriftliche Frage 25 des Abgeordneten Andrej Hunko auf Bundestagsdrucksache 19/8434 wird verwiesen.

14. Was ist der Bundesregierung über die Weiterentwicklung von Europol zu einem „Exzellenzzentrum“ für die Entschlüsselung von Datenträgern oder gespeicherten Kommunikationsinhalten bekannt, wozu die EU-Kommission 5 Mio. Euro für die Polizeiagentur bzw. die Gemeinsame Forschungsstelle JRC bewilligt hat und weitere 500.000 Euro für Trainings mit der Europäischen Polizeiakademie und der European Cybercrime Training and Education Group (ECTEG) finanziert (vgl. Bundestagsdrucksache 19/7227), und für welche Bereiche oder Maßnahmen (auch Forschung) werden weitere Mittel gefordert oder vorgeschlagen?

EUROPOL wurden in 2018 insgesamt 5 Mio. Euro für den Aufbau einer Decryption-Plattform bereitgestellt. Der Decryption-Service wird allen MS der EU nach Maßgabe der Europol-Verordnung und Drittstaaten im Rahmen bestehender Abkommen zur Verfügung stehen.

15. Was ist der Bundesregierung über Ziele und Teilnehmende eines „Dark Web team“ bei Europol bekannt (Ratsdokument 10991/19), und wie haben sich Bundesbehörden an dessen Aufbau beteiligt?

Das bei EC3 Ende 2018 eingerichtete DarkWeb-Team besteht nach Kenntnis der Bundesregierung aus Analysten und unterstützt Experten der MS, die mit der Durchführung von Untersuchungen im Dark Web betraut sind.

16. Auf welchen völkerrechtlichen Rechtsgrundlagen will die Bundesregierung Hintertüren (manipulierte Software-Artefakte) ausnutzen, die in kritischen Infrastrukturen anderer Staaten vorhanden sind (vgl. Bundestagsdrucksache 19/11920, Antwort zu Frage 12)?

    a) Wurden diese Hintertüren bereits für Cyberangriffe durch die Bundesregierung genutzt oder werden diese vielmehr für die Reaktion auf zukünftige Bedrohungen bereitgehalten?

    b) Befinden sich diese Hintertüren lediglich in Software deutscher Hersteller oder nutzt die Bundesregierung auch entsprechende Zugänge über manipulierte Software-Artefakte ausländischer Firmen bzw. bereitet sie eine solche Nutzung vor?

Die Fragen 16 bis 16b werden aufgrund ihres inhaltlichen Zusammenhangs gemeinsam beantwortet.

Es wird auf die Antwort der Bundesregierung zu den Fragen 1 bis 3 der Kleinen Anfrage der Fraktion der FDP auf Bundestagsdrucksache 19/5472 verwiesen.

17. Was ist der Bundesregierung bekannt, wann die Verhandlung eines Abkommens zwischen der EU und den USA über den grenzüberschreitenden Zugang zu elektronischen Beweismitteln im Rahmen des „CLOUD-Act“ begonnen hat, welche Treffen hierzu bereits stattgefunden haben, welche weiteren Treffen geplant sind oder aus welchen Gründen sich diese Verhandlungen eventuell. verzögern (Ratsdokumente 10128/19 und ADD1)?

Nach Kenntnis der Bundesregierung ist die EU-Kommission, nachdem ihr im JI-Rat im Juni 2019 das Verhandlungsmandat erteilt wurde, in Vorbereitungsgespräche für die geplanten formellen Verhandlungen zu dem angestrebten EU-USA-Verwaltungsabkommen zur Erhebung elektronischer Beweismittel mit den zuständigen Arbeitseinheiten des US-Justizministeriums eingetreten.

Ein Gespräch auf Ministerebene zu dieser Thematik hat am 19. Juni 2019 im Rahmen der Ministertagung Justiz und Inneres in Bukarest stattgefunden; ein Treffen zwischen Kommissarin Věra Jourová und US-Justizminister William Barr wurde hierzu am Vortag abgehalten. Die EU-Kommission hat mitgeteilt, dass, nachdem die Aufnahme formeller Verhandlungen in Ermangelung einer Mandatierung auf US-Seite bislang noch nicht habe erfolgen können, nunmehr ein Verhandlungsmandat dort vorliege. Die erste Verhandlungsrunde sei für den 25. September anberaumt. Die Bundesregierung hat keine Kenntnis über die Terminierung weiterer Verhandlungsrunden.

18. Trifft es nach Kenntnis der Bundesregierung zu, dass sich die EU-Polizeiagentur Europol mit Möglichkeiten des polizeilichen Zugangs zu Kommunikation mit Ende-zu-Ende-Verschlüsselung befasst („[…] a possible approach to allow law enforcement to deal with for end-to-end encryption“; vgl. Ratsdokument 10991/19)?

Erforschung und Entwicklung von Fähigkeiten zur Entschlüsselung und das Vorhalten entsprechender Kapazitäten im Rahmen des Mandats stellt grundsätzlich eine wichtige Aufgabe von Europol dar. Vor dem Hintergrund steigender Komplexität und wachsender Herausforderungen, z. B. im Bereich der Verschlüsselung oder der IT-Forensik, trägt eine solche Forschung und Entwicklung durch die EU-Polizeiagentur EUROPOL zur ressourcenschonenderen Entwicklung gemeinsamer Lösungen bei. Auf die Antwort zu Frage 14 wird verwiesen.

Gesamtherstellung: H. Heenemann GmbH & Co. KG, Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin, www.heenemann-druck.de
Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0722-8333