Deutscher Bundestag **Drucksache 19/13291**

19. Wahlperiode 18.09.2019

Kleine Anfrage

der Abgeordneten Andrej Hunko, Christine Buchholz, Dr. André Hahn, Niema Movassat, Thomas Nord, Petra Pau, Tobias Pflüger, Alexander Ulrich, Kathrin Vogler und der Fraktion DIE LINKE.

EU-Krisenreaktionsprotokoll für grenzüberschreitende Cyberangriffe

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 (EU) 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“.

Wir fragen die Bundesregierung:

1. Welche Details kennt die Bundesregierung zum „EU Law Enforcement Emergency Response Protocol“ für „erhebliche grenzüberschreitende Cyberangriffe“, und wie ist sie daran beteiligt?
2. Welche Konsequenzen ergeben sich durch das LE ERP für Bundesbehörden, und wie werden diese umgesetzt?
3. Welche Bundesbehörden sind dabei für welche Routinen des LE ERP zuständig (siehe Vorbemerkung der Fragesteller)?
4. Mithilfe welcher vorhandenen technischen Verfahren soll das LE ERP die schnelle Bewertung eines Vorfalls gewährleisten, und welche weiteren Fähigkeiten sollen hierzu aufgebaut werden?

5. Inwiefern kann hierzu nach Maßgabe der Europol-Verordnung auch auf militärische Erkenntnisse zurückgegriffen werden, etwa aus den Mitgliedstaaten oder der NATO?
6. Welche Details kennt die Bundesregierung zu den geplanten „operationellen Aktionsplänen für die Strafverfolgung“ nach einem Cyberangriff?
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)?
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?
9. Welche gemeinsamen Ermittlungsgruppen sind nach Kenntnis der Bundesregierung im Rahmen des LE ERP geplant?
10. Welche gemeinsamen Aktionstage (auch „Cyber patrol actions weeks“) plant Europol zu kriminellen Cyberaktivitäten, und wann sollen diese stattfinden?
    a) Welche weiteren Partner, etwa Drittstaaten, Interpol, regionale Initiativen, Expertennetzwerke oder Firmen und Institute nehmen an den Maßnahmen teil?
    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?
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?
12. An welchen derartigen Trainings haben welche 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?
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?
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?

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?

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)?

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)?

Berlin, den 21. August 2019

Dr. Sahra Wagenknecht, Dr. Dietmar Bartsch und Fraktion

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