Deutscher Bundestag **Drucksache 17/11341**

17. Wahlperiode 07. 11. 2012

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Andrej Hunko, Herbert Behrens, Ulla Jelpke, weiterer Abgeordneter und der Fraktion DIE LINKE.
– Drucksache 17/11100 –

Gemeinsame internationale Übung „Cyber Europe 2012“ mit Behörden, Banken und Internetdienstleistern

Vorbemerkung der Fragesteller

Am 4. Oktober 2012 hat die Europäische Agentur für Netz- und Informationssicherheit (ENISA) zum zweiten Mal die Übung „Cyber Europe“ ausgerichtet. Im Gegensatz zur gleichnamigen Übung 2010 sollen diesmal auch „Experten von Großbanken, Telecom-Unternehmen und Internetprovidern“ auf einen fiktiven Cyberangriff reagieren (heise.de, 4. Oktober 2012). 60 Banken waren beteiligt. 25 Länder haben an der Übung teilgenommen, vier weitere waren als Beobachter präsent. Ziel war die Erprobung und Zusammenschaltung nationaler und europäischer Cyberinfrastrukturen der Behörden und Telekommunikationsanbieter. Laut einer Mitteilung von ENISA sei die diesjährige Übung gegenüber 2010 in ihrem Ausmaß ebenso wie in ihrer Komplexität gewachsen (www.enisa.europa.eu/media/news-items/cyber-europe-2012-2013-first-results-show-success). Weitere Ziele werden mit „Testeffektivität und Skalierbarkeit der existierenden Mechanismen, Methoden und des Informationsflusses für die Kooperationen öffentlicher Behörden in Europa“ angegeben. Zudem sollen „Sicherheitslücken und Herausforderungen für einen effektiveren Umgang mit umfangreichen Internetstörfällen“ gefunden werden. Als Szenario wurde eine gezielte „Distributed Denial of Service“-Offensive auf „Online-Dienste in allen teilnehmenden Ländern“ angenommen, die durch weitere „ernsthafte Bedrohungen“ angereichert wurde. Derart protestiert etwa die Aktivistengruppe „Anonymous“ regelmäßig gegen nationale oder internationale Behörden und Firmen. Insgesamt wurden laut ENISA mehr als 1 000 als „Injektionen“ bezeichnete „Internetstörungen“ simuliert.

In Veröffentlichungen der ENISA findet sich kein Hinweis auf die weitere Zusammenarbeit mit den USA, die auch dieses Jahr Teile ihrer regelmäßigen Übung „Cyber Storm“ ausgeführt hatten. Auf Fragen zur Beteiligung deutscher Stellen an den zivil-militärischen Inhalten und Akteuren hatte die Bundesregierung mit dem Textbaustein „An dem Strang von Cyber Storm III, an dem Deutschland beteiligt war, haben keine militärischen Stellen teilgenommen“ geantwortet (Antwort der Bundesregierung auf die Kleine Anfrage der Fraktion DIE LINKE. auf Bundestagsdrucksache 17/7578). In der Auswertung der

---

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern vom 2. November 2012 übermittelt.

Die Drucksache enthält zusätzlich – in kleinerer Schrifttype – den Fragetext.

Übung „Cyber Storm III“ wurde verabredet, zukünftig weitere gemeinsame Übungen mit Mitgliedstaaten der EU abzuhalten. Dazu wurde eine „High-level EU-US Working Group on cyber security and cybercrime“ eingerichtet. Unter anderem hat die Arbeitsgruppe 2011 eine Übung der EU und der USA „Cyber Atlantic“ ausgerichtet.

1. Welche europäischen Länder waren an der „Cyber Europe 2012“ aktiv beteiligt, und welche hatten eine beobachtende Position inne?

Alle EU-Mitgliedstaaten mit Ausnahme von Bulgarien, Litauen, Polen, Malta und Großbritannien waren an der Übung aktiv beteiligt, zudem nahmen die Schweiz, Norwegen und Island an der Übung teil.

a) Welche weiteren Stellen des öffentlichen und privaten Bereichs waren beteiligt (bitte insbesondere die beteiligten Firmen und Banken aufführen)?

In Deutschland war das BSI für den öffentlichen Bereich beteiligt. Aus der Privatwirtschaft waren zwei große Banken und drei große Informations- und Kommunikationstechnologieanbieter (darunter die Deutsche Telekom AG und 1&1) beteiligt. Die anderen Unternehmen haben keine Erlaubnis erteilt, ihre Namen in Verbindung mit der Übung zu nennen.

b) Welche Aufgabe erfüllte das zentrale Lagezentrum der ENISA in Athen?

Mit „zentralem Lagezentrum“ ist die zentrale Übungssteuerung gemeint. Von hier aus wurden der Fortschritt der Übung beobachtet und Einlagen des Szenarios (Injects) an die Teilnehmer verschickt. Auch steuerte sie die Auswertung der Übung.

c) Inwieweit waren die „Computer Emergency Response-Teams“ (CERT) des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und der Bundeswehr in die Übung eingebunden?

Das CERT des Bundesamts für Sicherheit in der Informationstechnik (BSI – Computer Emergency Response Team für Bundesbehörden) war in die Übung eingebunden, die Bundeswehr war nicht beteiligt.

d) Welche weiteren CERT waren mit welchen Aufgaben integriert?

In Deutschland waren zum Teil die Unternehmens-CERTs der beteiligten Unternehmen eingebunden.

e) Welche Aufgaben übernahm das CERT der EU?

Das CERT.EU übte seine Aufgaben im Rahmen seiner Zuständigkeit für die EU-Einrichtungen.

2. Mit welchem Ziel haben deutsche Behörden an der Übung „Cyber Europe 2012“ teilgenommen?

Ziel war es, das IT-Krisenmanagement bei einer europaweiten IT-Krise zu üben. Der Schwerpunkt lag auf der Erprobung der gemeinsamen internationalen Krisenkommunikation.

a) Mit welchen Kräften waren öffentliche und private Teilnehmer aus Deutschland beteiligt?

Der personelle Aufwand bei den privaten Teilnehmern ist der Bundesregierung nicht bekannt. Auf Seiten des Bundes waren neun Mitarbeiter des BSI an der Übung beteiligt.

b) Worin bestand der Beitrag der Bundesnetzagentur bei der Übung?

Die Bundesnetzagentur hat nicht an der Übung teilgenommen.

c) Welche Kosten sind der Bundesregierung bei der Teilnahme entstanden, und aus welchen Etats wurden sie bestritten (bitte unter Angabe des prozentualen Anteils an den Gesamtkosten)?

Der Bundesverwaltung sind bei der Teilnahme geschätzte Kosten von ca. 25 000 Euro entstanden. Sie wurden aus dem Etat des BSI bestritten.

3. Wie war die Übung strukturell angelegt?

In der fiktiven IT-Krise kommunizierten staatliche Einrichtungen in den Mitgliedstaaten der Europäischen Union (EU) miteinander, um die Krise zu bewältigen. Diese Einrichtungen kommunizierten wiederum mit jeweils benannten nationalen Ansprechpartnern aus der Privatwirtschaft.

a) Welche Szenarien wurden für die Übung angenommen und durchgespielt?

Das Szenario simulierte Angriffe auf Server im Internet. Die Angriffe wurden mittels „Distributed Denial of Service“-Angriffen durchgeführt. Die Mitgliedstaaten mussten koordiniert handeln, um die angreifenden Systeme zu deaktivieren.

b) Worin bestanden die über 1 000 „Injektionen“?

Ein „Inject“ (deutsch: Einlage) ist die Einspielung eines Handlungselements im Gesamtszenario. So wird beispielsweise einem Übenden mitgeteilt, dass Angriffe auf ein Webangebot stattfinden.

c) Inwieweit berücksichtigte die Übung auch „cyberterroristische Anschläge“ oder sonstige über das Internet ausgeführte Angriffe auf kritische Infrastrukturen sowie Proteste, wie massenhafte E-Mails oder Proteste von „LulzSec“, „Anonymous“ oder ähnlichen Gruppen?

In der Übung wurden politisch motivierte Cyberangriffe auf Internetseiten von Banken mit dem Ziel der Störung von Diensten (Onlinebanking) simuliert. Hierzu wurde eine fiktive Organisation eingeführt, die diese Angriffe ausführt.

d) Auf welche Weise wurde den in Frage 3c erfragten Protesten begegnet, und wie wurden diese Maßnahmen in der Evaluation der Übung bzw. sonstigen Auswertungen bewertet?

Die Mitgliedstaaten mussten die angreifenden Server koordiniert außer Betrieb nehmen. Dabei wurde insbesondere die internationale Koordination als erfolgreich bewertet.

4. Wie wurde die „Cyber Europe 2012“ geplant und vorbereitet?

Die Planung wurde von der Europäischen Agentur für Netz- und Informationssicherheit (ENISA) koordiniert. Eine Arbeitsgruppe mit Teilnehmern aus den EU-Mitgliedstaaten steuerte die Planung.

a) Wer gehörte einer diesbezüglichen Planungsgruppe an, und von wem wurde diese initiiert?

Aus Deutschland war ein Mitarbeiter des BSI Mitglied in der Planungsgruppe. Die Planungsgruppe existiert schon seit der Planung der Cyber Europe 2010.

b) Inwieweit wurden hierzu 2010 und 2012 welche Beratungsunternehmen mit welchen Aufgaben eingebunden?

ENISA hat bei beiden Übungen Beratungsunternehmen (2012: Fa. Crisisplan) eingebunden. Diese entwickelten eine Internetplattform für die Übungssteuerung. Die Unternehmen waren bei der Durchführung der Planungsgruppenbesprechungen beteiligt und erstellten Unterlagen (z. B. Einlagen bzw. Injects s. o.) für die Übung.

5. Welches Szenario liegt der diesjährigen „Länderübergreifenden Krisenmanagementübung“ LÜKEX zugrunde?

Im Jahr 2012 wird keine LÜKEX (Kurzwort für Länderübergreifende Krisenmanagementübung) durchgeführt. LÜKEX-Übungen finden in der Regel im zweijährigen Rhythmus statt.

a) Wann soll die nächste LÜKEX stattfinden, und wer bereitet diese vor?

Die nächste LÜKEX findet am 27. und 28. November 2013 statt und wird durch das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) im Zusammenwirken mit dem Robert Koch-Institut (RKI), dem Bundesinstitut für Risikobewertung (BfR) und dem Bundesamt für Verbraucherschutz und Lebensmittelsicherheit (BVL) unter Federführung der zuständigen obersten Bundesministerien vorbereitet. Die Übung LÜKEX 13 behandelt das Thema „Außergewöhnliche biologische Bedrohungslagen“.

b) Welche Bundesministerien, Bundesbehörden, Hilfsorganisationen, Verbände und Wirtschaftsunternehmen werden daran teilnehmen, und worin besteht ihre Aufgabe?

An der Übung LÜKEX13 werden das Bundesministerium des Innern (BMI), das Bundesministerium für Ernährung, Landwirtschaft und Verbraucherschutz (BMELV), das Bundesministerium für Gesundheit (BMG), das Bundesministerium der Verteidigung (BMVg) und das Bundesministerium der Finanzen (BMF), einschließlich der zuständigen Geschäftsbereichsbehörden intensiv beteiligt sein. Weitere betroffene Bundesressorts sind das Auswärtige Amt (AA) und das Bundesministerium für Verkehr, Bau und Stadtentwicklung (BMVBS). Fachlich werden auch das Presse- und Informationsamt der Bundesregierung (BPA), das Bundesministerium für Wirtschaft und Technologie (BMWi) und das BMF betroffen sein. Ferner werden sich neun Bundesländer an der Übung beteiligen. Die Auswahl der beteiligten Verbände und Unternehmen sowie der Hilfsorganisationen ist derzeit noch nicht abgeschlossen. Die LÜKEX-Übungen simulieren mit einem realistischen Szenario besondere Lagen, in denen die Beteiligten ihr Zusammenwirken im jeweiligen originären Aufgabenbereich üben.

c) Welche ausländischen privaten oder öffentlichen Stellen sind in die Übung integriert oder beobachten diese?

Eine Beteiligung von internationalen Akteuren (z. B. Europäische Kommission, European Food Safety Authority oder des European Centre for Disease Prevention and Control) ist aufgrund der bestehenden internationalen Meldewege vorgesehen.

d) Inwieweit berücksichtigt die Übung auch „cyberterroristische Anschläge“ oder sonstige über das Internet ausgeführte Angriffe auf kritische Infrastrukturen sowie Proteste, wie massenhafte E-Mails oder Proteste von „LulzSec“, „Anonymous“ oder ähnlichen Gruppen?

LÜKEX ist eine Übungsserie, die verschiedenste Themen des Krisenmanagements aufgreift. Szenarien aus dem Cyberraum sind nicht Gegenstand der LÜKEX 2013.

e) Auf welche Weise wurde den in Frage 5d erfragten Protesten begegnet, und wie wurden diese Maßnahmen in der Evaluation der Übung bzw. sonstigen Auswertungen bewertet?

Die in Frage 5d erfragten Proteste sind nicht Gegenstand der LÜKEX 2013.

6. Welche europäischen Länder waren an der „Cyber Atlantic 2011“ (www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cyber- atlantic/cyber-atlantic-2011) aktiv beteiligt, und welche hatten eine beobachtende Position inne?

Es waren Österreich, Belgien, Tschechien, Estland, Finnland, Frankreich, Deutschland, Ungarn, Irland, Italien, Niederlande, Rumänien, Slowakei, Spanien, Schweden und Großbritannien beteiligt. Es nahmen einige weitere Länder auf Einladung der EU sowie das Aufbauteam des CERT-EU als Beobachter teil.

a) Welche weiteren Stellen des öffentlichen und privaten Bereichs waren beteiligt (bitte insbesondere die beteiligten Firmen und Banken aufführen)?

Aus Deutschland waren neben dem BMI und dem BSI keine weiteren Stellen, also auch keine Firmen und Banken, beteiligt.

b) Welche Aufgaben übernahmen die ENISA und das damals provisorische CERT der EU bzw. vergleichbare Strukturen?

ENISA übernahm die Rolle des „Gastgebers“. Sie steuerte und unterstützte die Planung, Vorbereitung, Durchführung und Nachbereitung der Übung. Das Aufbauteam von CERT.EU war als Beobachter bei der Übung anwesend.

c) Mit welchem Ziel haben deutsche Behörden an der Übung „Cyber Atlantic 2011“ teilgenommen?

Deutsche Übungsziele waren:

– Überprüfung und Weiterentwicklung der Verfahren der multinationalen Zusammenarbeit bei IT-Krisen und der
– Austausch von bewährten Praktiken in der multinationalen Zusammenarbeit bei IT-Krisen.

d) Mit welchen Kräften waren öffentliche und private Teilnehmer aus Deutschland beteiligt?

Deutschland war mit drei Mitarbeitern aus der Bundesverwaltung beteiligt.

e) Worin bestand der Beitrag der Bundesnetzagentur bei der Übung?

Die Bundesnetzagentur wurde während der Vorbereitung der Übung zur Berücksichtigung ihrer gesetzlichen Aufgaben national eingebunden.

f) Welche Kosten sind der Bundesregierung bei der Teilnahme entstanden, und aus welchen Etats wurden sie bestritten (bitte unter Angabe des prozentualen Anteils an den Gesamtkosten)?

Der Bundesverwaltung sind bei der Teilnahme geschätzte Kosten von ca. 5 000 Euro entstanden. Sie wurden aus dem Etat des BMI (33 Prozent) bzw. des BSI (66 Prozent) bestritten.

7. Wie war die „Cyber Atlantic 2011“ strukturell angelegt?

Die Übung war eine Planbesprechung von IT-Krisenmanagementrepräsentanten mit durch Besprechungen simulierter Kommunikation zu Verfahren und Prozessen der multinationalen (EU) und transatlantischen IT-Krisenzusammenarbeit in einem Tagungszentrum der EU in Brüssel.

a) Welche Szenarien wurden für die Übung angenommen und durchgespielt?

Es wurden zwei Szenarien angenommen: Ein „Advanced Persistence Threat“ (APT)-Angriff gegen nationale Computer- und Netzsicherheitsbehörden der Teilnehmer mit dem Abfluss und der Veröffentlichung sensibler Informationen, zudem ein Angriff gegen Prozesssteuerungssysteme von Windkraftanlagen und von anderen Kritischen Infrastrukturen.

b) Inwieweit berücksichtigte die Übung auch „cyberterroristische Anschläge“ oder sonstige über das Internet ausgeführte Angriffe auf kritische Infrastrukturen sowie Proteste, wie massenhafte E-Mails oder Proteste von „LulzSec“, „Anonymous“ oder ähnlichen Gruppen?

Für das erste Szenario wurde als Angreifer eine Hackergruppe mit „Anonymous ähnlichem“ Hintergrund angenommen und im zweiten Szenario wurde die Reaktion auf Angriffe gegen kritische Infrastrukturen geübt.

c) Auf welche Weise wurde den in Frage 7b erfragten Protesten begegnet, und wie wurden diese Maßnahmen in der Evaluation der Übung bzw. sonstigen Auswertungen bewertet?

Bei der Übung wurde wie in der Antwort zu Frage 7 dargestellt das multinationale Zusammenspiel zur Abwehr der Angriffe und zur Bewältigung der IT-Krise gespielt. Die Verfolgung der Angreifer spielte eine nachgeordnete Rolle. Die Maßnahmen der Zusammenarbeit wurden als zweckmäßig bewertet.

8. Wie wurde die „Cyber Atlantic 2011“ geplant und vorbereitet?

   Wer gehörte seitens der EU oder ihrer Mitgliedstaaten einer diesbezüglichen Planungsgruppe an, und welche Aufgaben wurden hierfür übernommen?

Die Übung wurde von einer Planungsgruppe aus der EU, den EU-Mitgliedstaaten und den USA geplant und vorbereitet.

Alle Übungsteilnehmer einschließlich ENISA nahmen auch an der Planungsgruppe teil (siehe auch die Antwort zu Frage 6). Hierbei galt es unter anderem die Idee der Übung, die Übungsziele, die Szenarien mit ihren Einlagenelementen sowie die organisatorischen Aspekte der Durchführung vorzubereiten.

9. Welche (auch virtuellen) Treffen der Unterarbeitsgruppe „Cybercrime“ des „EU-/US-Senior- Officials-Treffen“ hat es 2012 gegeben, und welchen Inhalt hatten diese?

Es wird davon ausgegangen, dass mit der Unterarbeitsgruppe Cybercrime eine Unterarbeitsgruppe der „EU-US Working Group on Cybersecurity and Cybercrime“ gemeint ist. Von einer Unterarbeitsgruppe Cybercrime des EU-/US-Senior-Officials-Treffen besitzt die Bundesregierung keine Kenntnis.

Bei der „EU-US Working Group on Cybersecurity and Cybercrime“ handelt es sich um ein Gremium, in dem auf Seiten der Europäischen Union nicht alle Mitgliedstaaten, sondern nur die Kommission, die jeweilige Präsidentschaft sowie das Ratssekretariat regelmäßig vertreten sind. Deutschland wird anlassbezogen zu Treffen dieser Arbeitsgruppe eingeladen.

Kenntnisse über Treffen und Inhalte der Unterarbeitsgruppe Cybercrime im Jahr 2012 liegen der Bundesregierung nicht vor.

10. Welche Regierungen von EU-Mitgliedstaaten sowie anderer Länder waren 2012 (auch als Beobachter) an Aktivitäten der US-Übung „Cyberstorm“ beteiligt (auch an etwaigen Auswertungen), die laut dem „Department of Homeland Security“ auch dieses Jahr andauert (www.dhs.gov/cyber-storm-securing-cyber-space)?

Deutschland ist im Jahr 2012 an den Vorbereitungen für einen, von der eigentlichen US-Übung getrennten, eigenständigen Strang von „Cyberstorm IV“ beteiligt. An der zurzeit laufenden Übungsvorbereitung unter Federführung der USA sind aus Europa neben Deutschland auch Finnland, Frankreich, die Niederlande, Norwegen, Schweden, die Schweiz, Ungarn und das Vereinigte Königreich sowie nichteuropäisch Australien, Kanada, Japan und Neuseeland beteiligt. Die tatsächliche Übung dieses Strangs von Cyberstorm IV wird im März 2013 stattfinden.

   a) Welche US-Ministerien bzw. -Behörden waren dieses Jahr an „Cyberstorm“ beteiligt?

An dem Strang von Cyberstorm IV, an dem Deutschland sich beteiligt, wird für die USA nur das Department of Homeland Security mit dem US-CERT teilnehmen.

b) Wie viele Angehörige welcher deutscher Behörden haben an welchen Standorten an den Aktivitäten zu „Cyberstorm“ teilgenommen?

An dem Strang von Cyberstorm IV, an dem Deutschland sich beteiligt, nimmt im Rahmen der Vorbereitung eine Mitarbeiterin des BSI in Bonn teil. Eine Dienstreise in die USA ist geplant.

c) Welche Kosten sind der Bundesregierung bei der Teilnahme entstanden?

Im Rahmen der Vorbereitung des Strangs von Cyberstorm IV, an dem Deutschland sich beteiligt, sind bislang geschätzte Kosten von ca. 3 000 Euro entstanden.

d) Was ist damit gemeint, wenn die Bundesregierung für 2010 von einer „dislozierte[n] Stabrahmenübung mit einem ‚Computerwurm‘-Szenario“ spricht (vgl. Bundestagsdrucksache 17/7578)?

Es wurden an verschiedenen Standorten bzw. in verschiedenen Ländern (= disloziert) Krisenstäbe ohne deren nachgeordneten ausführenden Anteile (= Stabsrahmenübung) mit einem Szenario zu einem sich schnell und selbstständig ausbreitenden Computerschadprogramm (= Computerwurm) konfrontiert. Diese mussten Entscheidungen treffen und vor allem bereichsübergreifende bzw. multinationale Abstimmungen zur IT-Krisenreaktion einleiten, ohne dass die konkrete Maßnahmendurchführung durch die nachgeordneten ausführenden Anteile geübt wurde (= Stabsrahmenübung).

11. Wie war das Verhältnis von zivilen zu staatlichen Akteuren bei Aktivitäten zu „Cyberstorm“ in diesem Jahr?

a) Welche privaten Firmen bzw. sonstigen zivilgesellschaftlichen Akteure haben daran teilgenommen?

An dem Strang von Cyberstorm IV, an dem Deutschland sich beteiligt, werden nach derzeitiger Planung keine nichtstaatlichen Akteure teilnehmen.

b) Wie bewertet die Bundesregierung die Trennung bei „Cyberstorm“ in einen militärischen und einen nicht-militärischen „Strang“ hinsichtlich einer Trennung polizeilicher und militärischer Belange?

An dem Strang von Cyberstorm IV, an dem Deutschland sich beteiligt, wird es keine Teilnahme von militärischen Kräften geben.

Eine Aufteilung in verschiedene Stränge erschwert das Üben der bereichsübergreifenden Zusammenarbeit nur, wenn als Übungsziel während der Übung die Trennung polizeilicher und militärischer Belange geübt werden soll. Ansonsten verfolgt jeder Teilnehmer seinen gesetzlichen Auftrag im Rahmen des jeweiligen Strangs.

Gesamtherstellung: H. Heenemann GmbH & Co., Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin, www.heenemann-druck.de
Vertrieb: Bundesanzeiger Verlagsgesellschaft mbH, 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