

Antwort der Bundesregierung

**auf die Kleine Anfrage der Abgeordneten Martina Renner, Dr. André Hahn,
Gökay Akbulut, weiterer Angeordneter der Fraktion DIE LINKE.
– Drucksache 19/3633 –**

Nationale und internationale Kooperationen des Bundesamtes für die Sicherheit in der Informationstechnik (BSI) (Nachfrage zu der Antwort der Bundesregierung auf die Kleine Anfrage auf Bundestagsdrucksache 19/3398)

1. Welche Produkte welcher Hersteller wurden dem in der Antwort zu Frage 13 beschriebenen Prozess der „Coordinated Vulnerability Disclosure“ (CVD) unterzogen?

Das BSI hat sich seit 2015 in vier Fällen mit deutschen Stellen zu Schwachstellen ausgetauscht. In einem Fall ging es um die sog. Efail-Schwachstellen in S/MIME und Open PGP. Hierzu fand im November 2017 ein Austausch mit Forschern der Fachhochschule Münster und der Ruhr Universität Bochum statt (vgl. BSI Pressemitteilung www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2018/efail-Schwachstellen15052018.html), um eine entsprechende Warnmeldung öffentlich bereitzustellen (vgl. „Efail“-Schwachstellen: Was Sie jetzt wissen sollten – <https://bsi-fuer-buerger.de/BSIFB/DE/Service/Aktuell/Informationen/Artikel/efailschwachstellen.html>).

Ein weiterer Fall betraf eine Schwachstelle der OSCI-Transportbibliothek in der Version 1.2 (www.xoev.de/sixcms/media.php/13/OSCI12_SecurityAdvisory_20170630.pdf).

Nach sorgfältiger Abwägung ist die Bundesregierung zu der Auffassung gelangt, dass die weitere Beantwortung der Frage 1 nicht in offener Form erfolgen kann. Zwar ist der parlamentarische Informationsanspruch grundsätzlich auf die Beantwortung gestellter Fragen in der Öffentlichkeit angelegt.

Eine Offenlegung der angefragten Informationen birgt jedoch die Gefahr, dass durch eine Veröffentlichung das Vertrauen der Hersteller in die Bundesregierung und der Quellenschutz des BSI substantiell gefährdet werden.

Ziel des „Coordinated Vulnerability Disclosure“ Prozesses ist es, Informationen von Herstellern über Schwachstellen zu gewinnen bzw. die Hersteller über Schwachstellen zu informieren, damit diese die Schwachstellen beheben, bevor sie öffentlich werden.

Grundlage dieses Prozesses ist die Vertraulichkeitszusage der Bundesregierung bspw. gegenüber Dritten oder Herstellern, ohne die sensible Informationen nicht erlangt werden könnten. Da in den anderen beiden Fällen eine Einwilligung der Hersteller zur Veröffentlichung nicht vorliegt, würde die Vertraulichkeitszusage durch Bekanntwerden der Information nicht eingehalten werden können und es bestünde die Gefahr, dass dem BSI zukünftig weniger oder keine Informationen aus dieser Richtung zugetragen werden, was seine Aufgabenerfüllung und damit die Sicherheit der Bundesrepublik Deutschland wesentlich gefährden würde. Deshalb sind die entsprechenden Informationen als Verschlusssache gemäß der VSA § 3 Nummer 2 als „VS – Geheim“ eingestuft. Daher wird hinsichtlich der weiteren Beantwortung dieser Frage auf den „VS-Geheim“ eingestuften Antwortteil verwiesen.*

2. Welche Kosten entstanden dem BSI durch diese CVD-Prozeduren?

Die CVD-Verfahren wurden im Rahmen der allgemeinen Aufgabenwahrnehmung des BSI bearbeitet. Es erfolgte keine Kostenbelastung von dedizierten Kostenträgern.

3. Wie hoch waren die Kosten, die die beteiligten Unternehmen trugen?

Der Bundesregierung liegen keine Erkenntnisse darüber vor, welche Kosten bei den beteiligten Unternehmen entstanden sind.

4. Wie verfahren die beteiligten Unternehmen mit dem Wissen um Sicherheitslücken nach Kenntnis der Bundesregierung?

Nach Kenntnis der Bundesregierung wurden die Schwachstellen bei den beteiligten Unternehmen im Rahmen der standardisierten Produktentwicklung behoben bzw. Workarounds aufgezeigt.

5. Folgt aus der in der Antwort zu Frage 20 enthaltenen Mitteilung, dass die internationale Zusammenarbeit des BSI „Im Wesentlichen [...] im Kontext und an den Standorten von Europäischer Union und NATO“ stattfindet, dass diese Zusammenarbeit auch Institutionen wie die Bundeswehr, ausländisches Militär oder EU- bzw. NATO-Institutionen umfasst und falls ja, welche Institutionen im Besonderen?

Die Zusammenarbeit des BSI mit EU- und NATO-Institutionen erfolgt im Rahmen gesetzlicher Aufgaben und Zuständigkeiten. Im Besonderen findet eine Zusammenarbeit des BSI mit EU-Institutionen wie dem Rat, der Kommission, der ENISA und der ESA statt. Im Hinblick auf die NATO sind es zivile Bereiche des North Atlantic Council (CDC, C3B) sowie des NATO HQ (Emerging Security Challenges Division).

Eine Zusammenarbeit des BSI mit der Bundeswehr findet bei EU- und NATO-Institutionen statt, falls BSI und Bundeswehr im Rahmen ihrer jeweiligen gesetzlichen Aufgaben und Befugnisse gemeinsam in Gremien vertreten sind. Im Besonderen betrifft dies das NATO „Security Products Evaluation and Certification

* Das Bundesministerium des Innern, für Bau und Heimat hat die Antwort als „VS – Geheim“ eingestuft.

Die Antwort ist in der Geheimschutzstelle des Deutschen Bundestages hinterlegt und kann dort nach Maßgabe der Geheimschutzordnung eingesehen werden.

Capability Team“ (SPEC CaT) und das „GALILEO Security Accreditation Panel“ (GSAP) der „Global Navigation Satellite System Supervisory Authority“ (GSA).

Informationen darüber, ob die entsandten Vertreter anderer Staaten in Gremien und Institutionen ausländischen Streitkräften zuzuordnen sind, liegen der Bundesregierung nicht vor. Im Übrigen wird auf die Antwort der Bundesregierung zu den Fragen 19 und 20 der Kleinen Anfrage der Fraktion DIE LINKE. auf Bundestagsdrucksache 19/3398 verwiesen.

Vorabfassung - wird durch die lektorierte Version ersetzt.

