Deutscher Bundestag **Drucksache 19/9903**

19. Wahlperiode 06.05.2019

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Katja Keul, Dr. Konstatin von Notz, Luise Amtsberg, weiterer Abgeordneter und der Fraktion BÜNDNIS 90/DIE GRÜNEN
– Drucksache 19/9461 –

Vertraulichkeit und Sicherheit der elektronischen Kommunikation im Bereich des Notariats

Vorbemerkung der Fragesteller

Als unabhängige Träger eines öffentlichen Amtes werden für die Beurkundung von Rechtsvorgängen und andere Aufgaben auf dem Gebiet der vorsorgenden Rechtspflege in den Ländern Notarinnen und Notare bestellt (§ 1 der Bundesnotarordnung – BNotO). Sie sind Träger eines öffentlichen Amtes in der Rechtspflege, sind unabhängig und mit ihren Beurkundungs-, Beratungs-, und Betreuungsaufgaben ein wesentliches Element der Rechtspflege in Staat, Wirtschaft und Gesellschaft. Demgemäß hat die Vertraulichkeit und Sicherheit der elektronischen Kommunikation im Bereich der Notare mit Millionen sensibler, höchstpersönlicher wie wirtschaftsbezogener Daten einen besonders hohen Stellenwert.

Die Bundesnotarkammer als Zusammenschluss der Notarkammern hat nach § 78 Absatz 1 Satz 2 Nummer 9 i. V. m. § 78n BNotO die gesetzliche Aufgabe der Einrichtung der besonderen elektronischen Notarpostfächer und u. a. der Unterstützung der elektronischen Kommunikation der Notare mit Gerichten, Behörden und sonstigen Dritten. Nach § 78n Absatz 2 BNotO hat die Bundesnotarkammer sicherzustellen, dass der Zugang zum besonderen elektronischen Notarpostfach nur durch ein sicheres Verfahren mit zwei voneinander unabhängigen Sicherungsmitteln möglich ist. Die Bundesnotarkammer kann unterschiedlich ausgestaltete Zugangsberechtigungen für Notare und andere Personen vorsehen. Das Bundesministerium der Justiz und für Verbraucherschutz (BMJV) regelt durch Rechtsverordnung die Einzelheiten der besonderen elektronischen Notarpostfächer, insbesondere u. a. Einzelheiten ihrer Einrichtung und der hierzu erforderlichen Datenübermittlung und ihrer technischen Ausgestaltung einschließlich ihrer Barrierefreiheit, der Zugangsberechtigung und der Nutzung (§ 78n Absatz 5 BNotO).

Die Staatsaufsicht über die Bundesnotarkammer führt das BMJV. Die Aufsicht beschränkt sich darauf, dass Gesetz und Satzung beachtet, insbesondere die der Bundesnotarkammer übertragenen Aufgaben erfüllt werden (§ 77 Absatz 2 BNotO).

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums der Justiz und für Verbraucherschutz vom 30. April 2019 übermittelt.

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

Auf die Mündlichen Fragen 42 und 43 für die Fragestunde des Deutschen Bundestages am 13. Februar 2019, die lauten „Ist der Bundesregierung ein Sicherheitsproblem beim elektronischen Rechtsverkehr im Notariat (XNotar/EGVP) bekannt, und wenn ja seit wann?“ sowie „Hat sich die Bundesregierung im Rahmen der Rechtsaufsicht über die Bundesnotarkammer in Sachen Sicherheit des elektronischen Rechtsverkehrs im Notariat (XNotar/EGVP) zu Aufsichtsmaßnahmen veranlasst gesehen, und wenn ja, was ist deren Gegenstand?“ antwortete das BMJV mit Schreiben vom 13. Februar 2019: „Ich möchte die Fragen 42 und 43 wegen des Sachzusammenhanges zusammen beantworten. Der Bundesregierung ist im Zusammenhang mit dem Softwareprodukt XNotar und dem Elektronischen Gerichts- und Verwaltungspostfach kein Sicherheitsproblem bekannt. Dementsprechend bestand auch kein Anlass für aufsichtsrechtliche Maßnahmen.“ (Plenarprotokoll 19/79).

Nach den der fragestellenden Fraktion vorliegenden Informationen ist diese Antwort so nicht zutreffend.

1. Ist der Bundesregierung ein – u. a. an Vertreter des BMJV, der Bund-Länder-AG IT-Standards in der Justiz, Vertreter des Bundesamtes für die Sicherheit in der Informationstechnik (BSI) und Vertreter der Bundesnotarkammer – gerichtetes Schreiben des Deutschen EDV-Gerichtstages e. V. vom 22. Januar 2019 bekannt, mit einer Einladung zu einer Besprechung am 14. Februar 2019 in den Räumen der Bunderechtsanwaltskammer, in dem es einleitend heißt: „Zurückreichend bis in die Tage vor dem letzten EDV-Gerichtstag im September 2018 werden unterschiedliche Standpunkte zur Sicherheit der elektronischen Kommunikation im Bereich der Notare geäußert….“?

2. Waren, und wenn ja, welche, Vertreter der Bundesregierung und ihr nachgeordneter Einrichtungen bei der in Frage 1 genannten Veranstaltung zugegen?

Die Fragen 1 und 2 werden zusammenhängend beantwortet.

Das in Frage 1 bezeichnete Schreiben ist der Bundesregierung bekannt. Mit ihm wurde von Seiten der Bundesregierung lediglich ein Vertreter des im Bundesministerium der Justiz und für Verbraucherschutz (BMJV) für das Elektronische Gerichts- und Verwaltungspostfach (EGVP) zuständigen Referats zu der Veranstaltung am 14. Februar 2019 eingeladen, der jedoch an dem Termin nicht teilgenommen hat, weil nach der Tagesordnung Fragen des EGVP nur am Rande betroffen waren. Von den der Bundesregierung nachgeordneten Einrichtungen hat ein Vertreter des Bundesamts für die Sicherheit in der Informationstechnik (BSI) teilgenommen.

3. Was war das Ergebnis der in Frage 1 genannten Veranstaltung (bitte anhand der TOP 2 und 3 der Tagesordnung der Veranstaltung im Einzelnen beantworten)?

4. Bestanden nach Kenntnis der Bundesregierung die in der in Frage 1 genannten Einladung unter TOP 2 beschriebenen Sicherheitsprobleme, bestehen diese fort oder sind sie nach Kenntnis der Bundesregierung mittlerweile behoben?

Die Fragen 3 und 4 werden zusammenhängend beantwortet.

Unter dem Tagesordnungspunkt 2 der Veranstaltung am 14. Februar 2019 wurden die nachfolgend aufgeführten Themen behandelt, wobei ein Ergebnisprotokoll gefertigt wurde, dessen Inhalt zusammengefasst wie folgt lautete:

a) Übermittlung der PIN für den privaten Schlüssel des Notars

Der Sachverhalt betraf die Vergangenheit. Bei der zentralen Speicherung handelte es sich um eine bewusste Designentscheidung der BNotK, die zum damaligen Zeitpunkt insbesondere der unkomplizierten Abwicklung der Postfachübergabe an den Amtsnachfolger diente und die auf der Grundlage einer Risikoanalyse getroffen wurde. Die neuen beN-Zertifikate wurden ausschließlich lokal generiert, es werden keine privaten Schlüssel zentral gespeichert. Mit der neuesten Version von „XNotar“ werden keine privaten Schlüssel übermittelt.

b) Authentisierung gegenüber der Schnittstelle bei der BNotK mittels Mitsendung eines Zertifikats mit öffentlichem Schlüssel ausreichend

Der beschriebene Sachverhalt ist im Design des EGVP so vorgesehen. Die Absenderangabe in der Visitenkarte hat keine Bedeutung für die Authentisierung. Es werden derzeit Maßnahmen abgestimmt, um nur noch authentifizierte Nutzer zum EGVP zuzulassen und weitere Möglichkeiten der Absicherung gegen eine „Absenderfälschung“ umzusetzen. Die dargestellte Möglichkeit der Absenderfälschung beim Versand über ein beN setzt voraus, dass der Angreifer sich innerhalb des Notarnetzes befindet und mit realen Zugangsdaten am System angemeldet ist. Dies ist bei der Risikobewertung zu berücksichtigen. Dass weder die Clientsoftware „Governikus Communicator“ noch „XNotar“ die EGVP-Rolle des Absenders anzeigen, erleichtert „Absenderfälschungen“. Die BNotK wird in Abstimmung mit der Justiz Möglichkeiten prüfen, um zukünftig eine möglicherweise missverständliche Darstellung der Bedeutung der Absenderangabe im Programm „XNotar“ zu vermeiden.

c) Denial of Service-Attacke durch einheitlichen Account und einfach zu erratenden Login-Namen möglich

Die dargestellte Möglichkeit ist derzeit nicht völlig auszuschließen.

d) Verwendung eines bereits abgelaufenen Zertifikats in allen SAML/SSO-Requests

Nach den Angaben der BNotK handelte es sich hierbei um einen Fehler, wobei das Zertifikat jedoch zwischenzeitlich ausgetauscht wurde.

e) SAFE-ID aller Notare mit einem Netzwerk-Sniffing-Tool auslesbar

Da es sich bei der SAFE-ID um ein öffentliches Datum handelt, wird übereinstimmend kein Problem gesehen.

f) Crawling von Notardaten im Notarverzeichnis möglich, da die Amtsträger-ID exponiert wird

Da die Amtsträger-ID ebenfalls öffentlich ist, wird auch dies übereinstimmend für unproblematisch gehalten.

g) Clients: Abruf von Nachrichten mit beschädigten Inhaltsdatencontainer bei jedem neuen Nachrichtenabruf

Es handelt sich um ein erwartetes Verhalten. Wie hiermit umzugehen ist, ist eine fachliche Entscheidung der einzelnen Client-Hersteller.

h) Keine Prüfung der Absender gegen den Verzeichnisdienst SAFE im gesamten ERV

Es handelt sich nicht um eine Protokoll-, sondern um eine Funktions- bzw. Darstellungsfrage der einzelnen Clients.

i) Nachrichtenversand durch jeden Bürger an jeden im Adressbuch aufgeführten Notar ohne vorherige Registrierung möglich

Es werden, wie bereits dargelegt, derzeit Maßnahmen abgestimmt, um nur noch authentifizierte Nutzer zum EGVP zuzulassen.

Der Tagesordnungspunkt 3 der Veranstaltung betraf ein Fazit, nach dem die Teilnehmer lediglich den vorstehend unter Buchstabe a dargestellten Punkt kontrovers beurteilten, während sie in allen anderen Punkten ein gemeinsames Verständnis erzielten. Es wurde festgehalten, dass alle Beteiligten die sie betreffenden Themen eigenverantwortlich zu bewerten und über ggf. daraus abzuleitende Maßnahmen zu entscheiden hätten.

Zu Buchstabe c kann noch ergänzt werden, dass das Problem bisher im EGVP noch nicht virulent geworden ist und zudem durch die vorbezeichnete in Abstimmung befindliche Authentifizierung noch einmal eine deutliche Verringerung des Risikos angestrebt wird. Darüber hinaus liegen der Bundesregierung zu den einzelnen Punkten keine weiteren wesentlichen Erkenntnisse vor.

5. War bzw. ist es nach Kenntnis der Bundesregierung insbesondere zutreffend,

   a) dass die Notare von jeder Person mit entsprechenden Kenntnissen durch einen sogenannten Denial-of-Service-Angriff aus dem System ausgesperrt werden können,

   b) dass sich die Notarpostfachlösung nicht an die gesetzlichen Vorgaben zur Nutzung zweier unabhängiger Sicherungsmittel hält,

   c) dass die PIN der Notare an Dritte übertragen wurde,

   d) dass u. U. die privaten Zertifikate der Notare an Dritte übertragen wurden,

   e) dass eine technische Möglichkeit der Entschlüsselung der Inhaltsdaten auf dem Transportweg bestand oder besteht?

Zu Frage 5a wird auf die Antwort zu den Fragen 3c und 4c verwiesen. Zu den Fragen 5c und 5d wird auf die Antwort zu den Fragen 3a und 4a verwiesen. Im Übrigen liegen der Bundesregierung zu den Fragen keine näheren Erkenntnisse vor.

6. Hat das BMJV zu dem Gegenstand dieser Anfrage den Rat des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit gesucht, wenn ja, wann, und mit welchem Ergebnis, wenn nein, warum nicht?

Das BMJV hat den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zum Gegenstand der Kleinen Anfrage nicht kontaktiert, weil dafür keine Veranlassung bestand. Die Einrichtung und der Betrieb des beN obliegen nach § 78n der Bundesnotarordnung (BNotO) der BNotK. Das BMJV führt nach § 77 Absatz 2 BNotO lediglich die Staatsaufsicht über die BNotK. Die Aufsicht beschränkt sich darauf, dass Gesetz und Satzung beachtet, insbesondere die der BNotK übertragenen Aufgaben erfüllt werden. Belastbare Anhaltspunkte dafür, dass die BNotK bei der Einrichtung und dem Betrieb des beN gegen datenschutzrechtliche Vorschriften verstoßen würde, lagen dem BMJV nicht vor.

7. Hat das BMJV zu dem Gegenstand dieser Anfrage den Rat des BSI gesucht, wenn ja, wann, und mit welchem Ergebnis, wenn nein, warum nicht?

Die für die Einrichtung und den Betrieb des beN zuständige BNotK und das BSI haben gemeinsam an der Veranstaltung am 14. Februar 2019 teilgenommen. Die BNotK hat somit den Rat des BSI eingeholt. Eine Veranlassung für das BMJV, darüber hinaus selbst ebenfalls noch das BSI zu kontaktieren, bestand nicht.

8. Hat das BMJV zum Gegenstand dieser Anfrage mit den für Notare zuständigen Landesaufsichtsbehörden bzw. Landesjustizverwaltungen kommuniziert, und wenn ja, wann, mit wem und mit welchem Inhalt?

Das BMJV hat zum Gegenstand der Kleinen Anfrage keinen Kontakt mit den für Notare zuständigen Landesaufsichtsbehörden/Landesjustizverwaltungen aufgenommen, weil dafür keine Veranlassung bestand.

9. Hat sich das BMJV zu dem Gegenstand dieser Anfrage anderweitigen Rat, zum Beispiel bei einer Beratungsfirma, eingeholt?

Wenn ja, wann, bei wem und mit welchem Ergebnis?

Das BMJV hat zum Gegenstand der Kleinen Anfrage auch keinen anderweitigen Rat eingeholt, weil dafür kein Bedarf bestand.

10. Welche gesetzlichen Meldepflichten sind für Fälle von IT-Sicherheitslücken gegenüber welcher Behörde potentiell einschlägig, und hat die Bundesregierung im vorliegenden Fall entsprechend das Vorliegen einer Meldepflicht geprüft, und wenn nein, warum nicht?

Meldepflichten bei Verletzungen des Schutzes personenbezogener Daten (Artikel 4 Nummer 12 der Datenschutz-Grundverordnung – DSGVO) ergeben sich aus den Artikeln 33 und 34 DSGVO. Für die BNotK und die Bundesregierung bestehen darüber hinaus im vorliegenden Kontext keine speziellen „Meldepflichten“ für Fälle von IT-Sicherheitslücken. Eine Veranlassung für Meldungen bestand daher nicht.

11. Sieht die Bundesregierung vor dem Hintergrund der Erfahrungen mit den bestehenden Rechtsnormen zur Meldepflicht bei Rechtsverstößen im Bereich von IT-Sicherheit und Datenschutz Bedarf zur Nachbesserung, wenn ja, in welcher Hinsicht, wenn nein, warum nicht?

Für Kritische Infrastrukturen sieht das IT-Sicherheitsgesetz von 2015 bereits Meldepflichten bei bestimmten IT-Sicherheitsvorfällen gegenüber dem BSI vor. Diese sollen im Zuge der laufenden Novellierung des IT-Sicherheitsgesetzes erweitert werden. Die Schaffung weiterer Meldepflichten bei IT-Sicherheitsvorfällen ist derzeit nicht vorgesehen.

Ob und inwiefern Änderungen an der DSGVO erforderlich sind, ist Gegenstand einer Evaluation der DSGVO. Diese Evaluation wird von der Europäischen Kommission verantwortet. Hinsichtlich des Verfahrens und Inhalts der Evaluation ist Artikel 97 DSGVO maßgeblich.

12. Seit wann sind welche Kosten nach Kenntnis der Bundesregierung für den Bund und die Bundesnotarkammer für das Programm XNotar bzw. das besondere elektronische Notarpostfach entstanden?

Bei dem Programm „XNotar“ handelt es sich um ein von der NotarNet GmbH vertriebenes Softwarepaket für den elektronischen Rechtsverkehr im Notariat. Erkenntnisse zu den Kosten dieses Programms liegen der Bundesregierung nicht vor.

Auf Seiten der Bundesregierung hat das BMJV die Einrichtung des beN insbesondere durch die Erarbeitung von Rechtsnormen in der BNotO sowie der Notarverzeichnis- und -postfachverordnung (NotVPV) begleitet. Die auf die Beschäftigung mit dem beN entfallenden Personalkosten der im BMJV tätigen Personen werden auf etwa 25 000 Euro geschätzt.

Das BSI ist im Rahmen seiner allgemeinen Beratungstätigkeit nur in geringem Umfang tätig geworden; die Kosten hierfür können nicht konkret beziffert werden.

Erkenntnisse darüber, welche Kosten das beN bei der BNotK hervorgerufen hat, liegen der Bundesregierung nicht vor.

13. War der Gegenstand dieser Kleinen Anfrage auch Gegenstand von Kontakten zwischen BMJV und Bundesnotarkammer, wenn ja, seit wann?

Der Punkt „Denial-of-Service-Angriff“ war bereits Gegenstand zweier Workshops der Arbeitsgruppe „IT-Standards in der Justiz“ am 13. Februar und 14. März 2018, an denen sowohl das BMJV als auch die BNotK teilgenommen haben. Im Übrigen hatte es zu den Gegenständen der Kleinen Anfrage keinen Kontakt zwischen dem BMJV und der BNotK gegeben.

14. Hat das BMJV im Rahmen der Staatsaufsicht jemals einen Bericht zu dem Gegenstand dieser Anfrage bei der Bundesnotarkammer angefordert, und wenn ja, wann, mit welchen Fragen, und mit welchen Antworten?

Das BMJV hat keinen solchen Bericht angefordert, da dafür keine Veranlassung bestand.

15. Seit wann sind nach Kenntnis der Bundesregierung der Bundesnotarkammer Sicherheitsprobleme beim Gegenstand dieser Kleinen Anfrage bekannt?

Der Punkt „Denial-of-Service-Angriff“ ist der BNotK nach Kenntnis der Bundesregierung spätestens seit Mai 2017 bekannt gewesen. Weiter war das BSI im Juni 2018 von Seiten der BNotK um eine Bewertung einiger der in der Veranstaltung vom 14. Februar 2019 behandelten Punkte gebeten worden, die damals aus Gründen fehlender Ressourcen und Zuständigkeiten nicht erfolgen konnte. Im Übrigen ist der Bundesregierung über die Erkenntnisse aus der Veranstaltung vom 14. Februar 2019 hinaus nicht bekannt, seit wann die den Gegenstand der Kleinen Anfrage bildenden Punkte der BNotK bekannt waren.

16. Sieht sich das BMJV qua Staatsaufsicht in der Pflicht, gesetzmäßige Zustände hinsichtlich der gesetzlichen Vorgaben zur Sicherheit der elektronischen Kommunikation im Bereich der Notare sicherzustellen, und wenn nein, warum nicht?

Die entsprechende Pflicht des BMJV folgt aus § 77 Absatz 2 BNotO.

17. Teilt die Bundesregierung die Auffassung, dass eine wirksame Ende-zu-Ende-Verschlüsselung eine datenschutzrechtliche Voraussetzung für die Einführung des elektronischen Rechtsverkehrs der Notare darstellt, und wenn nein, warum nicht?

Nach Artikel 5 Absatz 1 Buchstabe f DSGVO müssen personenbezogene Daten in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit“). Die Ende-zu-Ende-Verschlüsselung ist hierbei eine mögliche technische Ausgestaltung (vgl. Artikel 32 Absatz 1 Buchstabe a DSGVO).

18. Handelt es sich nach Auffassung der Bundesregierung beim besonderen elektronischen Notarpostfach um eine echte Ende-zu-Ende-Verschlüsselung?

Abgesehen davon, dass keine feststehende Definition einer „echten Ende-zu-Ende-Verschlüsselung“ besteht, ist eine solche weder in der BNotO noch in der NotVPV als Voraussetzung für die Einrichtung des beN normiert. Für die Bundesregierung besteht daher keine Veranlassung, die Funktionsweise des beN im Hinblick auf diese Frage zu bewerten.

19. Wann und ggf. welche Auditierungen zur IT-Sicherheit und zur Einhaltung der gesetzlichen Vorgaben zum Gegenstand dieser Kleinen Anfrage hat das BMJV durchführen lassen?

Das BMJV hat keine entsprechenden Auditierungen durchführen lassen, da dafür keine Veranlassung bestand.

Satz: Satzweiss.com Print, Web, Software GmbH, Mainzer Straße 116, 66121 Saarbrücken, www.satzweiss.com
Druck: Printsystem GmbH, Schafwäsche 1-3, 71296 Heimsheim, www.printsystem.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