

18. Wahlperiode

Schriftliche Anfrage

des Abgeordneten **Sven Kohlmeier (SPD)**

vom 19. Mai 2020 (Eingang beim Abgeordnetenhaus am 20. Mai 2020)

zum Thema:

E-Mailverkehr außerhalb des Berliner Landesnetzes: Darf BürgerIn nicht mehr mit dem Amt mailen?

und **Antwort** vom 04. Juni 2020 (Eingang beim Abgeordnetenhaus am 08. Jun. 2020)

Senatsverwaltung für Inneres und Sport

Herrn Abgeordneten Sven Kohlmeier (SPD)
über
den Präsidenten des Abgeordnetenhauses von Berlin

über Senatskanzlei - G Sen -

Antwort

auf die Schriftliche Anfrage Nr. 18/23 533

vom 19. Mai 2020

über E-Mailverkehr außerhalb des Berliner Landesnetzes: Darf BürgerIn nicht mehr mit dem Amt mailen?

Der Senat ist sich des Stellenwerts des Fragerechts der Abgeordneten bewusst und die Beantwortung Schriftlicher Anfragen der Mitglieder des Abgeordnetenhauses nach Artikel 45 Absatz 1 der Verfassung von Berlin hat eine sehr hohe Priorität. Gegenwärtig konzentriert der Senat seine Arbeit und seinen Ressourceneinsatz aber auf die Bekämpfung der infektionsschutzrechtlichen Gefährdungslage für die Berliner Bevölkerung. Vor diesem Hintergrund beantworte ich Ihre Schriftliche Anfrage im Namen des Senats von Berlin wie folgt:

1. Welche Dienstanweisungen zum Umgang mit dem E-Mailverkehr außerhalb des Berliner Landesnetzes (d.h. von Behörden des Landes Berlins zu Email-Adressen wie zB. BürgerInnen) gibt es in den einzelnen Bezirken und wer war an der Erstellung der Dienstanweisungen beteiligt (aufgeschlüsselt nach Bezirk)?

Zu 1.:

Bei der IKT-Steuerung des Landes Berlin liegen keine umfassenden Daten über Art und Umfang von bezirksspezifischen Dienstanweisungen zum Umgang mit dem E-Mailverkehr außerhalb des Berliner Landesnetzes aus den einzelnen Bezirken vor. Gleiches gilt für Informationen über die Beteiligung bei der Erstellung etwaiger Dienstanweisungen. Es gelten die allgemeinen Regelungen zum Umgang mit dem E-Mailverkehr (s. zu 3.)

2. Welche Unterstützung erfolgt bei der Erstellung der Dienstanweisungen zum Umgang mit dem E-Mailverkehr außerhalb des Berliner Landesnetzes durch die Senatsverwaltung und wie wird die Unterstützung abgerufen (aufgeschlüsselt nach Bezirk)?

Zu 2.:

Es besteht keine explizite Unterstützung für die Erstellung der Dienstanweisungen zum Umgang mit dem E-Mailverkehr außerhalb des Berliner Landesnetzes durch die Senatsverwaltung.

3. Welche allgemeinen Weisungen zum Umgang mit E-Mailverkehr außerhalb des Berliner Landesnetzes gibt es durch die Senatsverwaltung?

Zu 3.:

Nach § 4 Absatz 2 E-Government-Gesetz ist jede vom Anwendungsbereich umfasste Behörde verpflichtet, auch eine De-Mail-Adresse im Sinne des De-Mail-Gesetzes sowie einen E-Mail-Zugang mit einer gängigen Ende-zu-Ende-Verschlüsselung, zum Beispiel PGP-Standard, zu eröffnen.

Weiterhin hat die Berliner Justiz den elektronischen Zugang zu allen Gerichten und Staatsanwaltschaften eröffnet. Beteiligte können bei den Gerichten und Staatsanwaltschaften des Landes Berlin Dokumente, insbesondere Schriftsätze, auch elektronisch einreichen. Elektronische Dokumente müssen entweder mit einer qualifizierten elektronischen Signatur der verantwortenden Person versehen sein oder von der verantwortenden Person signiert und über einen sicheren Übermittlungsweg eingereicht werden. Sichere Übermittlungswege sind das besondere elektronische Anwaltspostfach (beA), das besondere elektronische Behördenpostfach (beBPo) oder eine absenderbestätigte DE-Mail. Rechtsgrundlagen sind §§ 130a ZPO, 14 FamFG, 46c ArbGG, 65a SGG, 55a VwGO, 52a FGO, 32a StPO, § 110c OWiG sowie § 753 ZPO.

Zudem können Klagen, Verfahrensanträge oder Schriftsätze in Gerichtsverfahren als elektronische Dokumente mit einer qualifizierten elektronischen Signatur der verantwortenden Person an das Elektronische Gerichts- und Verwaltungspostfach des Gerichts oder der Staatsanwaltschaft rechtswirksam eingereicht werden. Die hierfür zugelassenen Sende- und Empfangskomponenten sind vorgegeben und veröffentlicht.

Daneben sehen die Prozessordnungen sichere Übermittlungswege vor. Bei der Nutzung eines sicheren Übermittlungsweges müssen die übermittelten Dateien nicht mit einer qualifizierten elektronischen Signatur versehen werden. Sichere Übermittlungswege sind derzeit:

- das besondere elektronische Anwaltspostfach für Rechtsanwälte (beA)
- das besondere elektronische Behördenpostfach für Behörden und juristische Personen des öffentlichen Rechts sowie (beBPo)
- die absenderauthentifizierte DE-Mail

4. Welche technischen Möglichkeiten und Tools zur sicheren Kommunikation zB mit PGP werden den Bezirksverwaltungen zur Verfügung gestellt ?

Zu 4.:

Sowohl in den Richtlinien der Berliner Regierungspolitik als auch im Berliner E-Government-Gesetz (EGovG Bln) ist der Wille zur elektronischen Abwicklung von Verwaltungsabläufen festgeschrieben. Dementsprechend wurden der Verwaltungskundschaft Möglichkeiten eröffnet, mit jeder Behörde elektronisch in Kontakt treten zu können.

E-Mails von Bürgerinnen und Bürgern, die von privaten E-Mail-Adressen versendet oder empfangen werden, sind allerdings in der Regel nicht verschlüsselt. Um eine direkte, formlose und sichere Kommunikation der Bürgerinnen und Bürger zu ermöglichen wurde De-Mail eingeführt - ein auf E-Mail-Technik beruhendes

Kommunikationsmittel zur sicheren, vertraulichen und nachweisbaren Kommunikation. Dieses wird mit der unter 3. dargestellten Verpflichtung zur Zugangseröffnung sichergestellt. Das IT-Dienstleistungszentrum Berlin (ITDZ) hat dazu im Auftrag der Senatsverwaltung für Inneres und Sport ein zentrales De-Mail-Gateway als Basisdienst De-Mail in Betrieb genommen. Damit ist es allen Behörden und Einrichtungen des Landes Berlin möglich, De-Mails mit Hilfe der eigenen E-Mail-Infrastruktur oder Fachverfahren zu versenden.

Die Einrichtung von De-Mail-Accounts ist für die Bürgerinnen und Bürger allerdings mit einem gewissen organisatorischen und finanziellen Aufwand verbunden. Der Bund und die übrigen Bundesländer haben das Thema nicht anders gelöst und bisher keine anderen Lösungen als das Land Berlin gefunden.

Aufgrund der Datenschutzanforderungen im Sinne der Verordnung (EU) 2016/679 (sog. Datenschutz-Grundverordnung) ist grundsätzlich die Verschlüsselung der elektronischen Kommunikation sicherzustellen. Diese sollte zumindest durch eine Transportverschlüsselung, wie sie der De-Mail-Dienst bietet, eingehalten werden.

5. Ist der Beantwortung vonseiten des Senats noch etwas hinzuzufügen?

Zu 5.:

Aus IT-strategischer Sicht wird ein von den Behörden bereitgestelltes Angebot zur Ende-zu-Ende verschlüsselten E-Mail-Kommunikation nur als ergänzendes Angebot für Bürgerinnen und Bürger betrachtet, das sich für eine formlose, gleichwohl als schutzbedürftig eingeschätzte Übermittlung von Informationen per E-Mail an die Verwaltung außerhalb verfügbarer E-Government-Verfahren eignet.

Sofern ein regelmäßiger Austausch von schützenswerten Daten im Rahmen einer Fachaufgabe notwendig ist, sind dazu die entsprechenden E-Government-Verfahren mit entsprechenden Sicherheitsfunktionen auszurüsten.

So bietet beispielsweise die Postfach-Komponente des Service-Kontos Berlin (SKB) eine anlassbezogene, strukturierte Kommunikation an. Aktuell können hier bereits Fachverfahren, die an dem SKB angebunden sind, Nachrichten zu dem jeweiligen Verwaltungsvorgang für die SKB-Nutzenden einstellen. Da der Zugriff auf das SKB-Postfach derzeit jedoch nur per Benutzername und Passwort erfolgt, dürfen hier wie bei einer normalen E-Mail keine Nachrichten mit einem hohen Schutzbedarf resp. mit personenbezogenen Daten eingestellt werden. Auch können die SKB-Nutzenden keine Nachrichten an das jeweilige Fachverfahren senden.

Perspektivisch ist vorgesehen, dass SKB-Nutzende nicht nur Nachrichten erhalten, sondern auch anlassbezogen an die am SKB angebundenen Fachverfahren versenden können. Ferner soll das SKB-Postfach Nachrichten mit einem hohen Schutzbedarf bereitstellen können, indem sich die Nutzenden auf einem höheren Vertrauensniveau am SKB anmelden können (z.B. durch die Nutzung der eID-Funktion des Personalausweises).

Eine umfassende und allgemeingültige Lösung für die Anforderung zum rechtssicheren Austausch von E-Mails mit Bürgerinnen und Bürgern außerhalb des Verwaltungsnetzes erfordert eine Public Key Infrastruktur (PKI) mit einem öffentlich anerkannten Wurzelzertifikat in Verbindung mit der Ausgabe der Zertifikate an alle Beschäftigten und der zusätzlichen Erstellung von Organisationszertifikaten möglich.

Alle anderen Lösungen stellen entweder einzelfallbezogene Sonderlösungen dar, erfüllen nicht die rechtlichen Anforderungen oder sind im täglichen Umgang nicht praktikabel.

Ein Projekt zur Einführung einer -den vorgenannten Anforderungen entsprechenden- Verwaltungs-PKI läuft bereits. Unter den derzeitigen geltenden personellen und finanziellen Rahmenbedingungen ist im positiven Fall, mit einem Projektergebnis, d.h. mit dem Beginn des Roll-Outs der Zertifikate, im Jahr 2023 zu rechnen.

Berlin, den 04. Juni 2020

In Vertretung

Sabine Smentek
Senatsverwaltung für Inneres und Sport