Chaos Computer Club

Chaos Computer Club Berlin e. V.
Postfach 64 02 36
10048 Berlin

S T E L L U N G N A H M E

an den Rechtsauschuß des Deutschen Bundestages

Elektronischer Rechtsverkehr

Gesetzentwurf zur Förderung des elektronischen Rechtsverkehrs mit den Gerichten

Linus Neumann
Berlin, 14. April 2013

Die vorliegenden Gesetzesentwürfe der Bundesregierung und des Bundesrates haben es sich zum Ziel gesetzt, die allgemeine Akzeptanz für den elektronischen Rechtsverkehr mit Gerichten und zwischen den Behörden und den Bürgern zu erhöhen.

Im Entwurf der Bundesregierung wird für die bisherige mangelnde Akzeptanz ein fehlendes Nutzervertrauen in die tatsächlichen und rechtlichen Rahmenbedingungen vermutet. Dafür wird einerseits die mangelnde Verbreitung der elektronischen Signatur sowie andererseits ein Mangel an tatsächlichen und rechtlichen Möglichkeiten zur Einreichung elektronischer Dokumente verantwortlich gemacht.[1]

Letzterem Umstand soll durch die Verpflichtung zur Schaffung entsprechender Angebote begegnet werden, was als hehres Ziel allgemein zu begrüßen ist. Der mangelnden Akzeptanz der qualifizierten elektronischen Signatur jedoch soll dadurch begegnet werden, dass minderwertige und sachfremde technische Verfahren qua Gesetz für sicher und angemessen deklariert werden. Von dieser Lockerung des Anspruchs an beweiskräftige Dokumente und Willensbekundungen ist entschieden abzuraten.

[1] BT-Drs. 17/12634, 6. März 2013, S.1: http://dip21.bundestag.de/dip21/btd/17/126/1712634.pdf

Mangelnde Verschlüsselung als Gefahr für die Nutzer

In der Stellungnahme des CCC zum Gesetz zur Förderung der elektronischen Verwaltung sowie zur Änderung weiterer Vorschriften[2] für den Innenausschuß des Deutschen Bundestag wurde bereits ausführlich dargelegt, daß das De-Mail-Verfahren bereits heute allgemein anerkannten und gängigen Sicherheitsansprüchen nicht genügt.

Die hohe Relevanz und Vertraulichkeit der per De-Mail versendeten Dokumente erhöht die Attraktivität der De-Mail-Server als Angriffsziele. Dem entsprechend zu erwartenden Angriffsvolumen steht aufgrund der mangelnden Ende-zu-Ende-Verschlüsselung kein adäquates Sicherheitskonzept entgegen.

Die eID-Funktion kann nicht zum »Signieren« verwendet werden

In den vorliegenden Entwürfen werden die technischen Verfahren zur Signatur, Identitätsfeststellung, Authentisierung und Willenserklärung in unzulässiger Weise vermischt. Der elektronische Personalausweis (nPA) bietet zwei in der Anwendung sehr ähnliche Funktionen, denen jedoch fundamental unterschiedliche technische Bedeutung zukommt:

1. Der elektronische Identitätsnachweis (eID) ist das elektronische Äquivalent zum Vorzeigen eines Ausweisdokuments. Dieses Vorzeigen erlaubt die einmalige Prüfung der Identität des Trägers, bietet dem Vertragspartner aber keinerlei Beweiswert gegenüber Dritten.

2. Die qualifizierte elektronische Signatur hingegen ist an ein Dokument gebunden und bestätigt dessen Authentizität und Integrität gegenüber Dritten. Als dem Dokument separat beigefügte Datei erlaubt sie auch Dritten eine spätere und wiederholte Prüfung der Echtheit der Signatur. Nach gegenwärtigem Stand der Technik

---

[2] Linus Neumann: Stellungnahme zum Gesetz zur Förderung der elektronischen Verwaltung, 20. März 2013, BT-Drs. 17(4)695 B: http://www.bundestag.de/bundestag/ausschuesse17/a04/Anhoerungen/Anhoerung29/Stellungnahmen_SV/Stellungnahme_02.pdf

übersteigen die Kosten zum Fälschen einer qualifizierten elektronischen Signatur bei weitem den damit zu erzielenden Gewinn. Folglich gilt die qualifizierte elektronische Signatur als das einzige derzeit zur Verfügung stehende adäquate Verfahren zur rechtssicheren Signatur einer Willensbekundung.

Dieser Unterschied spiegelt sich auch im Gesetz über Rahmenbedingungen für elektronische Signaturen (SigG) wider.

Die von der Bundesregierung vorgeschlagene Änderung von § 690 der Zivilprozeßordnung sieht vor, daß Mahnanträge und Anträge auf Erlaß eines Vollstreckungsbescheids durch die elektronische Identifizierungsfunktion des elektronischen Personalausweises signiert (sic!) werden können. Eine Signatur mittels eID ist allerdings technisch ebenso unmöglich wie auch unangemessen für eine Willensbekundung.

Für jedes Dokument, das im Schriftverkehr einer Unterschrift bedarf, und insbesondere für eine Willenserklärung ist die qualifizierte elektronische Signatur das einzige derzeit zur Verfügung stehende und technisch angemessene Verfahren.

De-Mail kann kein qualifiziert elektronisch signiertes Dokument ersetzen

Die von der Bundesregierung vorgeschlagene Änderung von § 371a der Zivilprozeßordnung sieht vor, daß De-Mails, die bei bestätigter sicherer Anmeldung gemäß § 5 Absatz 5 mit einer elektronischen Signatur des Anbieters (und nicht des Nutzers) versehen sind, gleicher Beweiswert zugesprochen werden soll, wie einer qualifizierten elektronischen Signatur. Als Begründung wird angegeben:

> »Dass De-Mail und qualifizierte elektronische Signatur vergleichbare Beweiswirkung haben, rechtfertigt sich auch aus der Tatsache, dass die Anforderungen an die Zuverlässigkeit und Fachkunde sowie die Gewährleistung technisch-organisatorischer Rahmenbedingungen bei De-Mail-Diensteanbietern und Zertifizierungs-

diensteanbietern der qualifizierten elektronischen Signatur gleich sind.«[3]

Im Folgenden wird dargestellt, weshalb diese Aussage aus drei Gründen nicht zutrifft.

1. Die Eröffnung des Kontos erfolgt mittels (elektronischem) Identitätsnachweis: Beim Eröffnen seines De-Mail-Kontos muß der Anwender einmalig seine Identität gegenüber dem Anbieter unter Beweis stellen. Dieser einmalige Identitätsnachweis geschieht durch das Vorzeigen des Personalausweises oder durch äquivalente technische Maßnahmen (eID). Allen angebotenen Verfahren ist gemein, daß sie nur einmalig stattfinden und ihnenkeinerlei Beweiswert gegenüber Dritten zukommt.

Sie bieten daher keine Grundlage für die Annahme, daß De-Mails nur vom Inhaber des Zugangs gesendet oder empfangen werden.

2. Beim Versenden einer De-Mail wird die Identität nicht geprüft: Es wurde korrekt erkannt, daß eine einfache Authentifizierung mittels Nutzername und Paßwort keine ausreichende Sicherheit bietet, da derartige Zugangsdaten leicht in die Hände Dritter geraten können. Das Bundesamt für Sicherheit in der Informationstechnik schlägt daher für eine »sichere Authentifizierung« gemäß § 4 (2) De-Mail-Gesetz das mTAN-Verfahren[4] vor, bei dem ein zusätzlicher Authentifizierungscode per SMS an den Nutzer gesendet und zur Anmeldung verlangt wird. Allein für dieses Verfahren sind bereits heute drei Angriffsszenarien bekannt:

a. Infektion des Telefons: Mit Hilfe eines Trojaners, der SMS-Inhalte an den Angreifer weiterleitet und auf Wunsch dem Nutzer nicht anzeigt, kann unbemerkt Zugang erlangt wer-

[3] BT-Drs. 17/12634, S. 42.

[4] Vgl. Sicherheitsmerkmale De-Mail: http://www.cio.bund.de/DE/Innovative-Vorhaben/De-Mail/Sicherheitsmerkmale/sicherheitsmerkmale_node.html

den. Vor diesem Angriff warnt das BSI bereits in seiner Pressemitteilung vom 4. März 2011.[5]

b. Abhören der SMS-Inhalte über die Funkschnittstelle. Vor derartigen Angriffen warnt das BSI seit 2003.[6]

c. Impersonierung: Das Empfangen der Inhalte ist darüberhinaus mittels einer illegalen Kopie der SIM-Karte oder durch fortgeschrittene Angriffe auf die GSM-Verschlüsselung möglich, bei denen der Angreifer sich mit einem zweiten Mobiltelefon gegenüber dem Netzbetreiber als das Opfer ausgibt. Auch derartige Angriffe beschreibt das BSI bereits in einer Studie aus dem Jahr 2001.[7]

Aufgrund der häufigen Verwendung der mTAN-Methode im Online-Banking finden alle drei oben skizzierten Angriffe bereits heute regelmäßig Anwendung bei Kriminellen.

Ferner ist zu betonen, daß in § 4 (2) De-Mail-Gesetz nur der Anmeldevorgang, nicht jedoch der Sendevorgang geregelt wird: Nach einmaliger Zwei-Faktor-Authentifizierung bei der Anmeldung können mehrere De-Mails ohne erneute Authentifizierung gesendet werden. Einem Angreifer bieten sich daher auch die klassischen Web-Angriffsvektoren, wie zum Beispiel zum Beispiel Cross-Site-Scripting- und Man-in-the-middle-Angriffe.

Eine erfolgreiche Anmeldung zum De-Mail-Konto ist also auch bei erfolgter Zwei-Faktor-Authentifizierung kein Nachweis für die Identität des Nutzers und nicht ausreichend, um einer per De-Mail versandten Willensbekundung Beweiskraft zu geben.

3. Eine De-Mail wird vom Provider signiert und hat daher keine Beweiskraft für eine Willensbekundung des Absenders: Erhält der An-

---

[5] BSI: Neue Schadsoftware liest mTAN-Nummern mit, 4. März 2011: https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2011/Onlinebanking_mTAN_04032011.html

[6] Vgl. BSI: GSM-Mobilfunk. Gefährdungen und Sicherheitsmaßnahmen, 2003: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/GSM/gsm_pdf.pdf

[7] Vgl. BSI: Kommunikation in GSM-Mobilfunknetzen, Abschnitt 3.5: https://www.bsi.bund.de/DE/Publikationen/Studien/anonym/kommunikationgsm.html

greifer mittels einer der oben skizzierten Methoden Zugriff auf das De-Mail-Konto des Opfers, besteht keine Möglichkeit, die Identität festzustellen. Dennoch wird eine ausgehende De-Mail nach der Übermittlung an den Provider von diesem qualifiziert elektronisch signiert. Dies wird im vorliegenden Entwurf der Bundesregierung als Begründung dafür angeführt, einem per De-Mail versendeten Dokument den gleichen Beweiswert wie einem mit einer qualifizierten elektronischen Signatur durch den Absender versehenen Dokument einzuräumen.

Der Provider kann jedoch lediglich bestätigen, daß ihm die De-Mail in dieser Form vorlag, allerdings nicht, ob diese auch vom vermeintlichen Absender verfaßt wurde. Analog zu einer Beglaubigung kann also für die Übereinstimmung von Vorlage und Kopie gehaftet werden, nicht jedoch für die Echtheit der Vorlage.

Durch den oben dargestellten Ablauf wird deutlich, wie ein Dokument die Beweiskraft einer qualifizierten elektronischen Signatur erlangt, ohne annähernd den technischen und juristischen Anforderungen zu genügen. Darüberhinaus sind einige der bereits heute nicht nur möglichen, sondern auch gängigen Angriffsszenarien skizziert.

Empfehlungen

Aus technischer Perspektive besteht dringender Nachbesserungsbedarf in folgenden Bereichen:

1. Ende-zu-Ende Verschlüsselung in allen Bereichen erzwingen

Eine Zulassung von Übermittlungen per De-Mail sollte erst erteilt werden, wenn Ende-zu-Ende-Verschlüsselung voreingestellter Teil des Standards geworden ist. Andernfalls bietet De-Mail aus technischer Perspektive keinen nennenswerten Zugewinn an Sicherheit gegenüber einer herkömmlichen E-Mail.

2. Vorgaben des Signaturgesetzes einhalten

Da mit der qualifizierten elektronischen Signatur ein Verfahren existiert, das dem aktuellen technischen Stand zur digitalen Signatur von Dokumenten entspricht, erscheint ein gezieltes Herbeiführen einer Kostensenkung durch den Ausbau dieses Verfahrens als offensichtliche und sinnvolle Handlungsalternative.

Im übrigen verweisen wir auf die Stellungnahme des CCC zum Gesetz zur Förderung der elektronischen Verwaltung sowie zur Änderung weiterer Vorschriften.[8]

---

[8] Linus Neumann: Stellungnahme zum Gesetz zur Förderung der elektronischen Verwaltung, 20. März 2013, BT-Drs. 17(4)695 B: http://www.bundestag.de/bundestag/ausschuesse17/a04/Anhoerungen/Anhoerung29/Stellungnahmen_SV/Stellungnahme_02.pdf