Dr. Astrid Schumacher, Projektleiterin De-Mail im BSI

De-Mail – Infrastruktur für sichere elektronische Kommunikation

Einleitung

De-Mail soll grundlegende Sicherheitsfunktionen für den elektronischen Nachrichtenaustausch wie Verschlüsselung, sichere Identität der Kommunikationspartner und Nachweisbarkeit (Versand-/Zustellnachweise) – die der heute genutzten E-Mail fehlen – einfach nutzbar und damit breit verfügbar machen. Das Projekt De-Mail (entstanden aus dem Projekt „Bürgerportale“) zielt auf die Einrichtung einer sicheren elektronischen Kommunikationsinfrastruktur für Bürger, Unternehmen und Verwaltung. Sie soll ohne viel Aufwand von all diesen in den vielfältigen Anwendungsbereichen genutzt werden können.[1]

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) ist für das Sicherheits- und Zertifizierungskonzept verantwortlich und betreut die technischen Rahmenbedingungen für die Umsetzung einer sicheren und damit vertrauenswürdigen Infrastruktur des De-Mail-Informationsverbundes. Realisiert und betrieben wird De-Mail von einem Verbund staatlich zugelassener (akkreditierter) und in der Regel privater Anbieter – den De-Mail-Providern.

Ausgangslage

Über 95 Prozent aller E-Mails werden in Deutschland unverschlüsselt versendet. Sie können ohne großen Aufwand auf ihrem Weg durch das Internet abgefangen, wie Postkarten mitgelesen und in ihrem Inhalt verändert werden. Absender und Empfänger können nie vollständig sicher sein, mit wem sie gerade kommunizieren und ob die gesendete E-Mail tatsächlich beim Empfänger angekommen ist. Zudem hat der Anteil von SPAM am E-Mail-Verkehr stark zugenommen. Auch das Ausspähen von Zugangsdaten zu E-Mail-Konten (Phishing) wird immer häufiger. Dies alles hat bislang den Durchbruch von E-Mails überall dort verhindert, wo es auf Vertraulichkeit (verschlüsselt), Verlässlichkeit (angekommen) und Verbindlichkeit (eindeutige Identität) ankommt, die zusammen wichtige Voraussetzungen für besseren (Selbst-)Datenschutz, Datensicherheit und die Gewährleistung von Rechtssicherheit sind. Am Markt existierende Lösungen haben sich nicht in der Fläche durchsetzen können, da diese häufig zusätzliche Installationen auf den Rechnern der Nutzer erfordern (Zertifikate, Kartenlesegerät, etc.). Als Weiterentwicklung der „einfachen“ E-Mail bietet De-Mail eine einfach zu nutzende Technologie, mit der sicher im Internet miteinander Nachrichten ausgetauscht werden können.

Grundlegende Sicherheitsfunktionen

Versender und Empfänger einer De-Mail sind nachvollziehbar. Versand- und Zustellnachweise können einfach erstellt werden (Einschreiben). De-Mails sind auf dem Transport verschlüsselt und können daher nicht von Dritten abgefangen und/oder verändert werden. SPAM wird wirksam verhindert, weil Absender von De-Mails über eine sichere Erstidentifizierung eindeutig bekannt sind. Phishing und Identitätsdiebstahl können ausgeschlossen werden, wenn sich Nutzer beispielsweise mit dem künftigen neuen Personalausweis oder mit einem auf dem Mobiltelefon basierten Verfahren (mobile TAN) bei De-Mail anmelden. Durch diese Sicherheitsfunktionen kann ein großer Teil der bislang noch auf Papier abgewickelten Geschäfts- und Verwaltungsprozesse mit De-Mail einfacher, schneller und von jedem Ort aus vollständig elektronisch erledigt werden.

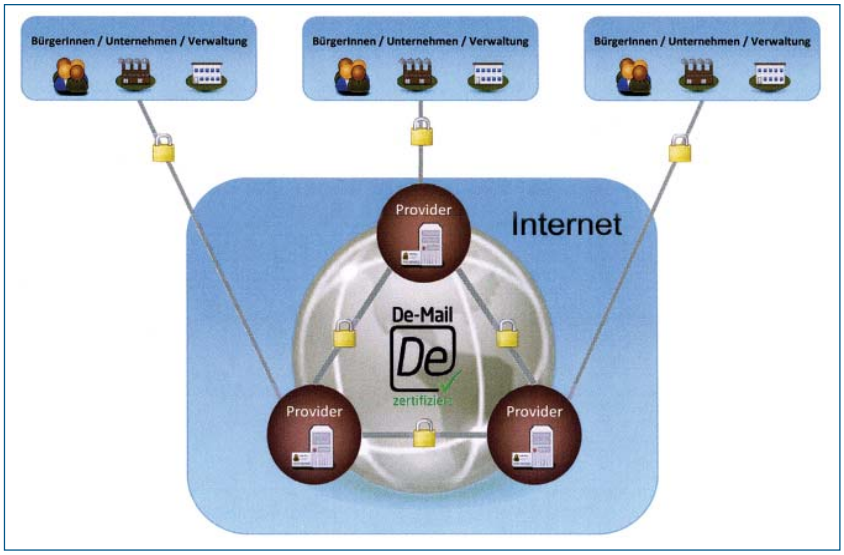
Einfache Handhabung

De-Mail-Konten können von Bürgerinnen und Bürgern ebenso wie von Unternehmen oder Behörden eröffnet werden. Sie müssen sich einmal zuverlässig identifizieren, z. B. mit dem Post-Ident-Verfahren, künftig auch mit dem neuen Personalausweis. Die Bedienung erfolgt im einfachsten Fall durch Webanwendungen, die in der Handhabung den bekannten Angeboten von E-Mail-Providern sehr ähnlich sind. Der Zugang zum De-Mail-Konto erfolgt über Nutzername/Passwort, über den neuen Personalausweis, mobiltelefonbasierte Verfahren (mobile TAN) oder andere sichere Verfahren. Unternehmen und Behörden können ihre existierenden E-Mail-Infrastrukturen über ein Gateway anschließen, sodass ihre Mitarbeiterinnen und Mitarbeiter die vorhandenen E-Mail-Clients wie gewohnt weiter verwenden können.

[1] Grundsätzlich zu De-Mail Dietrich/Keller-Herder, DuD 2010, S. 299 ff.; Stach, DuD 2008, S. 184 ff.; allgemeine Informationen zu De-Mail unter www. bsi.bund.de/de-mail

Vertrauen durch Sicherheit und Zertifizierung

Wesentlich für den Erfolg von De-Mail ist, dass die Diensteanbieter die Sicherheit, die sie versprechen, auch tatsächlich gewährleisten. Die Vertrauenswürdigkeit der Diensteanbieter ist entscheidende Voraussetzung für das berechtigte Vertrauen der Nutzer.[2] Ziel ist es, potenziellen Anbietern zu ermöglichen, ein angemessenes Sicherheitsniveau zu erreichen, gleichzeitig aber genügend Spielraum für die individuelle Gestaltung der Einsatzumgebung zu lassen.



Sicherer Kommunikationsraum.

Der De-Mail-Gesetzentwurf[3] bietet ein entsprechendes Nachweisverfahren für die Diensteanbieter an und sieht vor, dass Unternehmen, die ihre Dienste im De-Mail-Verbund anbieten wollen, auf Antrag eine staatliche Akkreditierung erhalten können.

Zu den Vorteilen, die die Akkreditierung mit sich bringt, gehört insbesondere der aus Sicht der IT-Sicherheit wesentliche Nachweis der geprüften Sicherheit, der für die Anbieter gegenüber den Nutzern auch marktstrategisch und werbewirksam verwertbar ist. Zudem knüpfen wesentliche Rechtsfolgen an die bestätigte Vertrauenswürdigkeit und finden damit ihre Grundlage nicht zuletzt in der Akkreditierung.[4]

Die Akkreditierung selbst ist an definierte Voraussetzungen geknüpft und wird von der zuständigen Behörde nur bei erfolgreichem Nachweis erteilt.[5] Mit der Akkreditierung erhalten die Anbieter zudem ein Gütezeichen, mit dem sie auf dem Markt für den von ihnen erbrachten Nachweis der umfassend geprüften technischen und administrativen Sicherheit ihrer Dienste werben dürfen.

Um akkreditiert zu werden, muss jeder Anbieter bestimmte technische, organisatorische und rechtliche Anforderungen erfüllen. Diese Anforderungen werden durch Technische Richtlinien des BSI (Anforderungskatalog/Regelwerk in Bezug auf Sicherheitseigenschaften und Funktionalität), IT-Grundschutz erweitert um De-Mail-spezifische Anforderungen sowie hinsichtlich des Datenschutzes in einem gesonderten Kriterienkatalog des Bundesbeauftragten für Datenschutz und Informationsfreiheit (BfDI) festgelegt und veröffentlicht. Daneben ist noch die auch sonst üblicher Weise im gewerblichen Bereich geforderte Zuverlässigkeit und Fachkunde, eine geeignete Deckungsvorsorge sowie weitere Pflichten etwa im Rahmen der De-Mail-Kontonutzung z. B. Aufklärungs- und Informationspflichten gegenüber dem Nutzer zu erfüllen.[6]

Ausblick

Die Vertrauenswürdigkeit der künftigen De-Mail-Dienste basiert auf einem sinnvollen System von Zertifikaten und Nachweisen, die ganz überwiegend (vom in dieser Form neuartigen Datenschutz-Nachweis abgesehen) auf bewährten Strukturen zur objektiven Prüfung und Bewertung von Informationsverbünden beruhen.

Die Feststellung der Vertrauenswürdigkeit der Anbieter durch eine behördliche Bestätigung macht schließlich den wesentlichen Unterschied zu anderen, möglicherweise in technischer Hinsicht vergleichbaren Angeboten aus.

Der vom De-Mail-Gesetzentwurf zur Verfügung gestellte gesetzliche Rahmen mit dem geschilderten technischen Unterbau bildet für das Ziel der geprüften sicheren Kommunikationsinfrastruktur die geeignete Architektur, innerhalb derer genügend Spielraum für die künftigen De-Mail-Provider bleibt, sich im Wettbewerb zu behaupten.

---

2 Vgl. dazu auch Roßnagel/Hornung/Knopp/Wilke, DuD 12/2009, S. 728 ff., S. 731, und Probst, DSB 2/2009, 16 ff.
3 BT-Drs 16/12598 vom 08. 04. 2009 (hier noch unter dem Begriff Bürgerportale); nachdem das Gesetz in der letzten Legislaturperiode nicht mehr verabschiedet werden konnte, wird kurzfristig ein überarbeiteter Entwurf in das parlamentarische Verfahren neu eingebracht; zuvor war ein Entwurf vom 02. 07. 2010 Grundlage für die Beteiligung der Länder und Verbände nach § 47 der Gemeinsamen Geschäftsordnung der Bundesregierung.
4 Vgl. zu den rechtlichen Aspekten Roßnagel/Hornung/Knopp/Wilke, DuD 12/2009, S. 728 ff., S. 731,
5 Als zuständige Behörde ist nach § 2 De-Mail-Gesetzesentwurf das BSI vorgesehen.
6 Vgl. zu den Voraussetzungen der Akkreditierung und Zertifizierung bei Schumacher, DuD 5/2010, S. 302–307.