Sicherheit bei De-Mail

Im Interview erklärt Dr. Frank Wermeyer, Geschäftsverantwortlicher für De-Mail bei der Deutschen Telekom, was den neuen Dienst so sicher macht, welche Vorkehrungen De-Mail-Provider für Datenschutz und -sicherheit treffen müssen und welche Pflichten die Sender einer De-Mail haben.

De-Mail gilt als elektronisches Pendant zur Briefpost. Wie sieht es denn in puncto Sicherheit aus?
Wermeyer: Unternehmen und Privatpersonen verschicken heute ganz selbstverständlich E-Mails – an Kunden, Geschäftspartner und Freunde. Doch wenn es darum geht, eine Rechnung einzureichen oder ein Angebot abzugeben, setzen viele aus Sicherheitsgründen noch immer auf die Briefpost. De-Mail ist dazu eine bequeme und sichere Alternative. Mit dem neuen Dienst bieten wir unseren Kunden eine einfache, gleichzeitig aber sichere und nachweisbare Möglichkeit zur nahtlosen elektronischen Kommunikation. Unsere Kunden können nicht nur auf die Seriosität der Telekom vertrauen. Als zertifizierter De-Mail-Anbieter unterliegen auch wir den strengen Anforderungen an Datensicherheit und -schutz aus dem De-Mail-Gesetz. Sicherheit entsteht bei De-Mail aus einem Paket unterschiedlichster Maßnahmen: verschlüsselte Transportkanäle und verschlüsselte Speicherung, eindeutig identifizierte Kommunikationspartner sowie abgesicherte Anmeldeverfahren.

Welche Pflichten haben die De-Mail-Provider?
Wermeyer: De-Mail dürfen nur Dienstleister anbieten, die hohe Sicherheits- und Datenschutzanforderungen erfüllen und in einem Prüfverfahren vom Bundesamt für Sicherheit in der Informationstechnik (BSI) zertifiziert werden. Dazu müssen sie alle Sicherheitsanforderungen aus dem De-Mail-Gesetz umsetzen und entsprechende technische und organisatorische Maßnahmen ergreifen. Das betrifft die eigene Systemumgebung, die Verbindung zu den Kommunikationspartnern sowie zu anderen De-Mail-Providern. Zum Beispiel muss der De-Mail-Anbieter während des Transports einer De-Mail sicherstellen, dass die Nachricht nicht mitgelesen werden kann und ihr Inhalt sich nicht verändern lässt.

Was tun die Provider, um die Daten und De-Mail-Systeme in ihren Rechenzentren zu schützen?
Wermeyer: Lassen Sie mich mit der äußeren Sicherheit beginnen. Alle De-Mail-Systeme sind nach ISO 27001 zertifiziert und befinden sich in Hochsicherheitsrechenzentren in Deutschland.

Dort sind die De-Mail-Server in gesicherten Räumen zunächst gegen die üblichen Gefahren aus Feuer, Hitze und Wasser besonders geschützt. Der Schutz vor Diebstahl und Manipulation wird dadurch gewährleistet, dass nur sehr wenige überprüfte Personen nur unter strengen Auflagen überhaupt Zutritt zu den Räumen haben. Genauso wichtig ist der Schutz vor Angriffen über das Internet von außen. Spezielle Firewalls und Anti-Viren-Programme schützen die Daten gegen derartige Angriffe. Weiterhin wird eine De-Mail, wenn sie auf dem Server des Providers eintrifft, verschlüsselt gespeichert. Selbst Wartungsarbeiten an De-Mail-Systemen können nur in einem besonders gesicherten Verfahren durchgeführt werden.

Zur Sicherheit zählen aber auch noch andere Aspekte: Alle Systeme und Dienste sind hochverfügbar, damit unsere Kunden De-Mail rund um die Uhr nutzen können. Dazu betreiben wir die Plattform in einer Geo-Redundanz, das heißt die Systeme laufen parallel in zwei räumlich getrennten Rechenzentren. Selbst ein Flugzeugabsturz auf eines der Rechenzentren würde nicht zu einem Ausfall des Dienstes führen. Jedes Rechenzentrum ist jeweils mit zwei getrennten Leitungen an das Netz angebunden. Fällt ein Verteilerknoten aus oder kappt ein Bagger bei Baumaßnahmen eine Leitung, lässt sich der Betrieb aufrechterhalten. Auch beim Personal gibt es strenge Vorschriften: Danach dürfen die De-Mail-Provider ausschließlich nachgewiesen fachkundiges und geschultes Personal einsetzen. Dazu gehört auch, dass wir die Vertrauenswürdigkeit unserer Mitarbeiter belegen müssen. Alle Kollegen, die mit dem Betrieb der Systeme betraut sind, müssen ein Führungszeugnis vorlegen. Und wir sind dazu verpflichtet, bestimmte Aufgabenbereiche strikt zu trennen. Ein Mitarbeiter, der beispielsweise für die Verschlüsselung der Daten verantwortlich ist, darf keinen Zugriff auf die verschlüsselten Daten haben.

Wie wird sichergestellt, dass die Provider die gesetzlichen Vorschriften einhalten?

Wermeyer: Nach der Akkreditierung zum De-Mail-Provider muss sich jeder Anbieter einmal jährlich einer Prüfung unterziehen und sich alle drei Jahre erneut vom BSI akkreditieren lassen. So stellt der Gesetzgeber sicher, dass die Provider in den wichtigen Maßnahmen nicht nachlassen und auch neue Sicherheitsanforderungen in ihr Sicherheitskonzept mit einbeziehen. Sollte der Verdacht auf Unregelmäßigkeiten bei einem Anbieter auftreten, kann das BSI natürlich als Aufsichtsbehörde jederzeit aktiv werden.

Kritiker bemängeln, dass durch den Wegfall der Ende-zu-Ende-Verschlüsselung die Sicherheit der Daten nicht durchgängig gewährleistet sei. Halten Sie diesen Einwand für gerechtfertigt?
Wermeyer: Nein, aus zwei Gründen. Das De-Mail-Gesetz schreibt vor, die Daten während des Transports von einem Protokoll auf ein anderes Protokoll umzuwandeln und auf Schadsoftware zu untersuchen. Das dauert wenige Tausendstelsekunden und geschieht rein maschinell innerhalb eines Hochsicherheitsrechenzentrums. Deshalb sehen wir hier auch nur ein theoretisches Risiko, dass die Daten dabei in falsche Hände geraten. Der andere Grund ist: Unternehmen und Privatpersonen, die noch höhere Anforderungen an die Sicherheit der Daten – zum Beispiel bei datenschutzrelevanten Informationen – stellen, können eine durchgehende Ende-zu-Ende-Verschlüsselung einrichten. Dabei wird der Inhalt der De-Mail durch den Versender verschlüsselt und erst durch den Empfänger wieder entschlüsselt. Weil die höchste Sicherheitsstufe – insbesondere für Privatpersonen – die Nutzung aufwendiger macht, wurde die Ende-zu-Ende-Verschlüsselung bewusst nicht zwingend vorgegeben. Das sicherste System bringt nichts, wenn es von den Bürgern nicht genutzt wird. Wir aber wollen mehr Sicherheit und damit Vertrauen bei der Nutzung des Internets erreichen.

Herr Dr. Wermeyer, vielen Dank für das Gespräch.

Kontakt:
Deutsche Telekom AG
Corporate Communications
Tel.: 0228 181 - 4949
E-Mail: medien@telekom.de