Kurzgutachten zum

Prüfungsbericht für den Datenschutz-Nachweis nach § 18 Abs. 3 Nr. 4 De-Mail-Gesetz

für die

T-Systems International GmbH
Hahnstraße 43d
60528 Frankfurt am Main

Sachverständige Prüfstelle (Recht und Technik):

intersoft consulting services AG
Frankenstraße 18a
20097 Hamburg
http://www.intersoft-consulting.de/

Prüfer und Verfasser: Rechtsanwältin Ann-Karina Wrede
awrede@intersoft-consulting.de

Rechtsanwalt Marcus Kirsch
mkirsch@intersoft-consulting.de

Leiter der Prüfstelle: Rechtsanwalt Matthias Lindner
mlindner@intersoft-consulting.de

Inhalt

1 Zeitpunkt und Ablauf der Prüfung

Die Prüfung für den Datenschutz-Nachweis nach § 18 Abs. 3 Nr. 4 De-Mail-Gesetz erfolgte im Zeitraum vom 02.01.2012 bis 29.02.2012 anhand von Dokumentensichtung und Prüfung, Interviews mit fachkundigem Personal sowie Ortsbesichtigungen an verschiedenen Standorten.
Gegenstand der Prüfung waren auch die Existenz und der Inhalt von Konzepten zum datenschutzgerechten Betrieb, da ein Produktivbetrieb erst nach dem Prüfverfahren aufgenommen werden darf.

Die datenschutzrechtliche Prüfung wurde auf Grundlage des De-Mail-Kriterienkataloges in der Version 1.2, des De-MailG, BDSG, TKG und TMG sowie weiterer datenschutzrechtlicher gesetzlicher Vorgaben sowie aufgrund der Technischen Richtlinien des BSI TR 01201 in der Version 1.00 durchgeführt.

2 Kurzbezeichnung

Am 03. Mai 2011 ist das De-Mail-Gesetz in Kraft getreten. Gemäß § 1 Abs. 1 De-Mail-Gesetz sind De-Mail-Dienste definiert als Dienste auf einer elektronischen Kommunikationsplattform, die einen sicheren, vertraulichen und nachweisbaren Geschäftsverkehr für jedermann im Internet sicherstellen sollen.
De-Mail-Dienste dürfen nur von solchen Diensteanbietern betrieben werden, die nach dem De-Mail-Gesetz akkreditiert worden sind. Dazu muss der Diensteanbieter bestimmte Anforderungen erfüllen, wozu unter anderem die Einhaltung technischer und organisatorischer Maßnahmen nach der Technischen Richtlinie des BSI TR 01201 und datenschutzrechtliche Anforderungen gehören.

Diesem Kurzgutachten liegt ein ausführliches Prüfgutachten für den Datenschutz-Nachweis nach § 18 Abs. 3 Nr. 4 De-Mail-Gesetz zugrunde. Dieses dient dem Nachweis der Einhaltung der datenschutzrechtlichen Kriterien. Auf Grundlage dieses Gutachtens wurde der T-Systems International GmbH (T-Systems)am 05.03.2012 durch den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) das für die Akkreditierung erforderliche Datenschutzzertifikat erteilt. Dieses Zertifikat bestätigt die Datenschutzkonformität der bei der T-Systems geplanten De-Mail-Dienste.

Die Veröffentlichung dieses Kurzgutachtens soll Transparenz für potentielle Nutzer erzeugen sowie darüber informieren, wie die De-Mail funktioniert, was das Gesetz im Hinblick auf den Datenschutz vorschreibt, wie diese Vorgaben bei der T-Systems umgesetzt worden sind und dass der BfDI mit der Erteilung des Zertifikates das Verfahren für datenschutzkonform befunden hat.

Die T-Systems wendet sich ausschließlich an Großkunden und bietet als wählbare Dienste den Postfach- und Versanddienst, den öffentlichen Verzeichnisdienst und das Accountmanagement an. Darüber hinausgehende freiwillige Dienste, wie die Dokumentenablage und der Identitätsbestätigungsdienst, sind nicht im Leistungsangebot enthalten.

3 Detaillierte Bezeichnung

3.1 Funktionsweise von De-Mail

Das Projekt De-Mail soll das verbindliche und vertrauliche Versenden elektronischer Nachrichten ermöglichen und stellt eine entsprechende Kommunikationsinfrastruktur für Bürger, sowie öffentliche und nicht-öffentliche Stellen dar. Neben der Nachweismöglichkeit über die Identität der Kommunikationspartner sowie der Zustellung der De-Mails soll der Dienst gewährleisten, dass Inhalte von De-Mails auf ihrem Weg durch das World Wide Web nicht mitgelesen oder manipuliert werden können.

Bei Geschäftskunden erfolgt die Kommunikation hauptsächlich über ein Gateway, welches die direkte Schnittstelle zu den Systemen der T-Systems bildet. Zusätzlich ist ein Zugriff der Kunden über ein Webfrontend auf den Account möglich, so dass ohne die Implementierung weiterer Software De-Mails versendet werden können. Der Zugriff auf den Account ist dabei mittels https verschlüsselt.

Es können verschiedene Bestätigungen, wie etwa Eingangs-, Versand- oder für bestimmte öffentliche Stellen die Abholbestätigung angefordert werden. Darüber hinaus wird der Zugang zum Account durch die Möglichkeit einer sicheren Anmeldung besonders geschützt. Im Gegensatz zur normalen Anmeldung mit Benutzernamen und Passwort erfordert die sichere Anmeldung Besitz und Wissen. Die sicherere Anmeldung kann entweder über den neuen Personalausweis oder das Mobil-TAN-Verfahren durchgeführt werden.

3.2 Vorgaben des Gesetzes

Der Kriterienkatalog, der als Grundlage der Prüfung sowie des erstellten Gutachtens diente, ist inhaltlich in vier Gruppen aufgeteilt:

- Rechtliche Zulässigkeit unter Angabe der rechtlichen Erlaubnistatbestände
- Dienstspezifische Umsetzung der technisch-organisatorischen Anforderungen einschließlich Verschlüsselung, Authentifizierung und Signaturen sowie Anforderungen an Datensparsamkeit
- Rechte der Betroffenen
- Einrichtung eines Datenschutzmanagementsystems

Die rechtliche Zulässigkeit richtet sich neben den allgemeinen datenschutzrechtlichen Vorgaben vor allem nach denen des De-Mail-Gesetzes, des Bundesdatenschutzgesetzes sowie des Telekommunikations-, Telemedien- und des Signaturgesetzes. Jede Erhebung, Verarbeitung oder Nutzung personenbezogener Daten bedarf demzufolge einer gesetzlichen Ermächtigungsgrundlage oder der ausdrücklichen Einwilligung des Betroffenen. Darüber hinaus sind die Grundsätze der Zweckbindung und der Datenlöschung nach Zweckfortfall zu beachten und für eine nahezu durchgängige dauerhafte Verschlüsselung des Transportes und der Speicherung der Daten zu sorgen.

Darüber hinaus ist die Umsetzung der technisch- und organisatorischen Anforderungen nach der Anlage zu § 9 BDSG sowie die Verarbeitung personenbezogener

Daten hinsichtlich Verschlüsselung, Authentifizierung und Signaturen sowie der Datensicherheit zu gewährleisten.

Ferner müssen Rechte der Betroffenen auf Benachrichtigung, Auskunft, Löschung oder Sperrung auf geeignetem Wege umgesetzt werden.

Schließlich muss auch ein Datenschutzmanagement im laufenden Betrieb implementiert sein, welches die Umsetzung der rechtlichen und technischen Vorschriften des Datenschutzes beinhaltet und insbesondere Wert auf die Einbeziehung des Datenschutzbeauftragten legt.

3.3 Umsetzung bei der T-Systems

Die datenschutzrechtlichen Vorgaben sind bei der T-Systems in geeigneter und erforderlicher Weise umgesetzt worden.

Es erfolgt ausschließlich eine Datenerhebung, -verarbeitung oder Nutzung auf Grundlage eines rechtlichen Erlaubnistatbestandes.
Die Verwendung personenbezogener Daten erfolgt ausschließlich in dem Maße, in dem diese für die Bereitstellung oder Erbringung von Leistungen des De-Mail-Dienstes erforderlich und notwendig sind. Der Nutzer wird über sämtliche Verarbeitungsschritte ausführlich informiert und entscheidet grundsätzlich selbst, welche Daten er angeben möchte und welche nicht.

Der Nutzer wird an verschiedenen Stellen über die Verwendung seiner Daten informiert: durch eine Datenschutzerklärung auf der Webseite, ein Hinweisblatt zum Datenschutz, auf dem Identblatt, während der Registrierung sowie in den AGB. Er erhält vor Beginn der Registrierung bei der T-Systems alle erforderlichen Informationen auf geeignete Weise.
Es erfolgte keine Verwendung der Daten durch Dritte. Alle Vertragspartner sind vertraglich auf die Einhaltung der gesetzlich vorgegebenen datenschutzrechtlichen Anforderungen verpflichtet.
Die für De-Mail angegebenen Daten werden nicht für den Adresshandel oder für Werbezwecke verwendet.

Darüber hinaus ist ein wirksamer und geeigneter Zugriffsschutz auf Nachrichten bzw. deren Inhalte etabliert. Die Nachrichten werden zu jedem Zeitpunkt auf verschlüsseltem Wege transportiert und ebenfalls jederzeit verschlüsselt abgelegt. Die Verschlüsselung ist hochwirksam und dem hohen Schutzbedarf angepasst.
Auch während der Überprüfung von Nachrichten auf Schadsoftware befinden sich die Nachrichten auf verschlüsselten Festplatten. Dadurch ist es auch den Mitarbeitern der T-Systems nicht möglich, auf Nachrichteninhalte zuzugreifen. Hierfür sind außerdem abgestufte Rollen- und Berechtigungskonzepte etabliert, die einen unbefugten Zugriff unterbinden. Diese gewährleisten den Zugriffs- und Zugangsschutz auf Systeme und Nutzerdaten.
Die Einhaltung der technischen Anforderungen wurde am 02.03.2012 bestätigt durch die Vergabe des ISO 27001-Zertifikates auf der Basis von IT-Grundschutz erweitert um Aspekte aus der Technischen Richtlinie TR 01201 De-Mail.

Zusätzlich sind alle Mitarbeiter der T-Systems auf das Daten- und das Fernmeldegeheimnis verpflichtet.

Darüber hinaus ist es den Nutzern möglich, mittels im Öffentlichen Verzeichnisdienst veröffentlichter und hinterlegter öffentliche Schlüssel eine Ende-zu-Ende-Verschlüsselung einzurichten. In diesen Fällen findet keine Überprüfung der Nachrichten auf Schadsoftware statt.
Die De-Mail-Systeme sind physikalisch von weiteren Systemen der T-Systems getrennt. Es erfolgt daher auch keine Vermischung von Datenbeständen.

Es sind feste Verfahren und Prozesse etabliert, welche die Umsetzung der Rechte der Betroffenen gewährleisten. Die Kontaktaufnahme mit dem Datenschutzbeauftragten ist über mehrere Eingangskanäle möglich.

Es ist ein Datenschutzbeauftragter bestellt, der in technische oder organisatorische Maßnahmen eingebunden ist und für eine konstante Sensibilisierung der Mitarbeiter sorgt, was sich auch im bestehenden Datenschutzmanagement zeigt. Darüber hinaus ist es den Nutzern in den meisten Fällen zusätzlich möglich, Änderungen oder Löschungen im eigenen Account selbst vorzunehmen. Die aus den verschiedenen Verfahrensbeschreibungen ersichtlichen technischen und organisatorischen Maßnahmen gewährleisten eine zweckgebundene Verwendung sowie eine fristgerechte und datenschutzkonforme Löschung der Daten.
Insgesamt zeigen die Mitarbeiter der T-Systems ein hohes Maß an Sensibilisierung für den Schutzbedarf von personenbezogenen Daten.

4 Zusammenfassung der Prüfergebnisse

Sämtliche Anforderungen des De-Mail-Kriterienkataloges, des Bundesdatenschutz-, des Telemedien-, des Telekommunikations- und des Signaturgesetzes sind erfüllt.

Durch verschiedene Maßnahmen, wie etwa den geregelten und kontrollierten Zutritt zu den Gebäuden der T-Systems als auch zu den genutzten Rechenzentren, kann von einer vorbildlichen Umsetzung der Zutrittskontrollen gesprochen werden. Auch die Zugangskontrollen zu den Systemen der T-Systems können als vorbildlich bezeichnet werden.

Insgesamt sind die von der T-Systems gewählten Maßnahmen geeignet, die datenschutzrechtlichen Aspekte der für De-Mail einschlägigen Gesetze zu erfüllen.

Während der Interviews und der Dokumentensichtung vor Ort hat sich stets der hohe Grad an Sensibilisierung der Mitarbeiter im Bereich Datenschutz und Datensicherheit gezeigt. Viele Aspekte werden als Selbstverständlichkeiten verstanden und entsprechend umgesetzt und im Betrieb gelebt.

5 Datenschutzfördernde Gestaltung

Die T-Systems hat zudem in einem Punkt eine datenschutzfördernden Gestaltung der De-Mail-Dienste ergriffen. So erfolgt nach einer fest definierten Zeit der Inaktivität ein automatisches Session-Logout.