Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Bonn, 1. März 2013

Handreichung
zum datenschutzgerechten Umgang mit besonders schützenswerten Daten beim Versand mittels De-Mail

Die Handreichung soll die Nutzer von De-Mail für die datenschutzrechtlichen Aspekte bei der Versendung besonders schützenswerter Daten mittels De-Mail sensibilisieren. Sie soll Hinweise für einen datenschutzgerechten Versand dieser Daten mittels De-Mail unter Berücksichtigung der Möglichkeit einer Ende-zu-Ende-Verschlüsselung geben, um damit zu einer rechtssicheren und weiten Verbreitung von De-Mail-Diensten beizutragen.

Am 3. Mai 2011 ist das De-Mail-Gesetz in Kraft getreten. Auf Grundlage dieses Gesetzes können sich Unternehmen akkreditieren lassen, um De-Mail-Dienste anzubieten. De-Mail-Dienste sind nach § 1 Abs. 1 De-Mail-Gesetz Telekommunikationsdienste auf einer elektronischen Plattform, die eine sichere, vertrauliche und nachweisbare Kommunikation für jedermann im Internet gewährleisten sollen. Die De-Mail ist letztlich eine besondere Form der E-Mail. Sie soll ohne zusätzliche Hard- und Software genauso einfach bedienbar sein, aber die Nachteile der E-Mail ausgleichen. Eine E-Mail kann nämlich mit geringem technischem Aufwand abgefangen, mitgelesen und verändert werden.

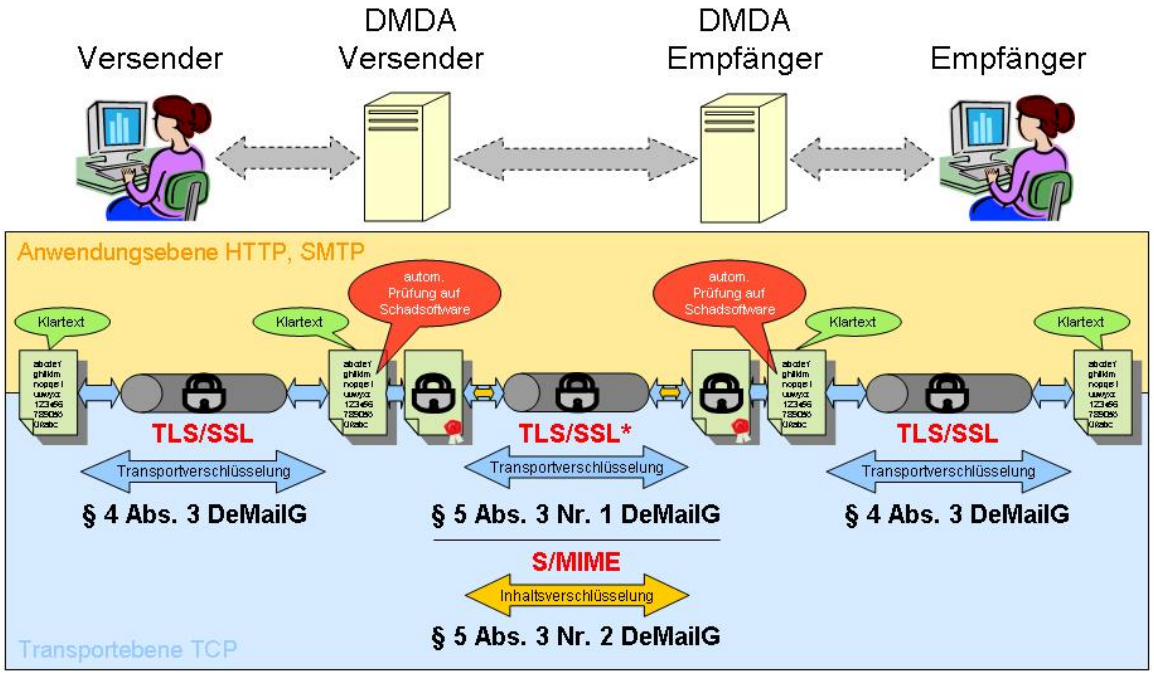
Das De-Mail-Gesetz stellt einerseits Anforderungen an Datenschutz und Datensicherheit beim De-Mail-Diensteanbieter (DMDA) und regelt andererseits, wie De-Mail für die rechtssichere elektronische Kommunikation eingesetzt werden kann. Dies bedingt einige Besonderheiten im Vergleich zur Nutzung von E-Mail-Diensten, so z.B. eine eindeutige Identifizierung vor der erstmaligen Nutzung von De-Mail. De-Mail bietet die Gewähr dafür, dass der Absender einer De-Mail zweifelsfrei ermittelt werden kann. Absende- und Eingangsbestätigungen, die mit einer qualifizierten elektronischen Signatur des DMDA versehen werden, bieten den sicheren Nachweis, dass die De-Mail versendet wurde und eingegangen ist. Schließlich wird die Nachricht durch den Anbieter transport- und inhaltsverschlüsselt.

Das De-Mail-Gesetz fordert:

- Der akkreditierte DMDA hat sicherzustellen, dass die Kommunikationsverbindung zwischen dem Nutzer und seinem De-Mail-Konto verschlüsselt erfolgt.
- Der Versand von einem DMDA zu jedem anderen DMDA muss über einen verschlüsselten gegenseitig authentisierten Kanal erfolgen.
- Der Inhalt einer De-Mail-Nachricht muss vom DMDA des Versenders zum DMDA des Empfängers verschlüsselt übertragen werden.

Die technischen Details lassen sich wie folgt zusammenfassen:

- Die Nachricht vom Versender an seinen DMDA und weiter vom DMDA des Empfängers an den Empfänger ist auf der Transportebene jeweils einfach durch Transportverschlüsselung gesichert (TCP + SSL/TLS). Die Authentisierung des Clients erfolgt automatisch mittels SSL-Handshake. Eine zertifikatsbasierte Clientauthentifizierung wird optional unterstützt.
- Die Nachricht ist zwischen dem DMDA des Versenders und dem DMDA des Empfängers doppelt gesichert: auf Anwendungsebene durch Inhaltsverschlüsselung und Signatur der Nachricht (S/MIME) sowie auf Transportebene durch Transportverschlüsselung (TCP + implizites1 SSL/TLS). Eine gegenseitige Clientauthentisierung muss zwingend zertifikatsbasiert erfolgen.
- Die Transportverschlüsselung (TLS) ist eine Punkt-zu-Punkt-Verschlüsselung (SSL-Handshake), weshalb die Nachricht nach dem Versand wieder unverschlüsselt vorliegt. Auf Transportebene liegt die Nachricht also in einem zufälligen Bitmuster vor, jedoch wäre sie auf Anwendungsebene ohne weiteres im Klartext zu lesen.
- Die Inhaltsverschlüsselung (S/MIME) ist eine Ende-zu-Ende-Verschlüsselung, wird aber gemäß TR De-Mail nur zwischen zwei DMDA gefordert.



§ 3 Abs. 4 Nr. 4 De-Mail-Gesetz sieht vor, dass der DMDA die De-Mail auf Befall mit Schadsoftware überprüfen muss. Vor dem Versand der Nachricht an den DMDA des Empfängers liegt diese beim DMDA des Versenders unverschlüsselt vor, so dass er sie zu diesem Zeitpunkt auf Schadsoftwarebefall hin prüfen kann. Anschließend leitet er die Nachricht zusätzlich zur Transportverschlüsselung inhaltsverschlüsselt an den DMDA des Empfängers weiter. Ist die Nachricht beim DMDA des Empfängers eingegangen, wird die Inhaltsverschlüsselung aufgehoben und die Nachricht wiederum auf Schadsoftwarebefall hin geprüft. Abschließend wird die Nachricht verschlüsselt im Postfach des Empfängers abgelegt. Nach jeder Prüfung wird die Nachricht in den Metadaten mit einem Hinweis versehen, ob die Überprüfung zu einem Befund geführt hat. Dieser Prüfprozess erfolgt zwar automatisiert auf Servern in einem Rechenzentrum des DMDA, das den Vorgaben des BSI entspricht. Zudem gibt es weitere technische und organisatorische Maßnahmen, die einen Zugriff durch einen Innen- wie auch einen Außentäter verhindern sollen. Gleichwohl besteht ein Restrisiko, dass insbesondere Administratoren des Anbieters vom Nachrichteninhalt Kenntnis nehmen.

Im Gegensatz dazu stellt die Ende-zu-Ende-Verschlüsselung eine durchgängige Verschlüsselung zwischen Versender und Empfänger dar und bietet sich daher für eine Versendung besonders schutzbedürftiger Daten an. Dies wird vom De-Mail-

Gesetz jedoch nicht gefordert. Für den DMDA ergeben sich dementsprechend keine Pflichten. Er darf den Versand Ende-zu-Ende-verschlüsselter Nachrichten lediglich nicht verhindern. Faktisch bedeutet dies, dass sich die Nutzer selbst um die Installation und Nutzung einer Verschlüsselungssoftware kümmern müssen. Eine Prüfung auf Schadsoftware kann der DMDA dann allerdings nicht durchführen. Problematisch ist zudem, dass Nachrichten nur dann verschlüsselt versendet werden können, wenn auch der Empfänger eine entsprechende Kryptografiesoftware einsetzt. Dies führt zu Verunsicherungen und Erschwernissen, die sich hätten vermeiden lassen, wenn die Ende-zu-Ende-Verschlüsselung zu den mit De-Mail bereitgestellten Standardmaßnahmen gehören würde.

Da die bisher akkreditierten DMDA für den Privatanwender bislang nur den Zugang per Web-Client ermöglichen, ist eine Ende-zu-Ende-Verschlüsselung für diesen derzeit kaum praktikabel. Der Versender muss die zu übermittelnde Nachricht auf seinem lokalen Rechner erstellen und mit einer Kryptografiesoftware verschlüsseln. Danach meldet er sich über den Web-Client an seinem De-Mail Konto an, erzeugt eine leere „Pseudo“-De-Mail und hängt dieser per Upload die verschlüsselte Datei an. Wirtschaftsunternehmen und die öffentliche Verwaltung haben es hier einfacher, da die Anbindung an De-Mail über ein Gateway erfolgt, d.h. im Firmen- bzw. Behördennetzwerk können normale E-Mail-Clients wie Outlook oder Lotus Notes genutzt werden, die von Hause aus eine Verschlüsselung unterstützen, so dass diese weitestgehend automatisiert erfolgen kann.

Es ist ein Grundsatz des Datenschutzes, dass bei der elektronischen Übertragung personenbezogener Daten die Integrität, Authentizität und Vertraulichkeit der Daten sichergestellt sein muss. Je schützenswerter ein Datum ist, desto strenger sind die technisch-organisatorischen Maßnahmen, die die verantwortliche Stelle einhalten muss. Bei bestimmten personenbezogenen Daten wie zum Beispiel Gesundheitsdaten, spielt besonders die Vertraulichkeit eine große Rolle. Unbefugte sollen in keinen Fall Kenntnis von diesen Daten erhalten. Bei der elektronischen Kommunikation wird die Vertraulichkeit dadurch gewährleistet, dass die Nachricht und ihre Anhänge mit einer geeigneten Software verschlüsselt werden. Betroffen sind hiervon alle besonders schutzbedürftigen personenbezogenen Daten, also solche, die potentiell eine besondere Sensibilität aufweisen. Dies gilt etwa für personenbezogene Daten an deren Verarbeitung und Nutzung besondere gesetzliche Anforderungen gestellt werden, wie z.B. die so genannten besonderen Arten personenbezogener Daten nach § 3 Abs. 9 BDSG oder die dem Sozialdatenschutz unterfallenden personenbezogenen Daten. Welche Schutzmaßnahmen für diese Daten angemessen sind, ergibt sich allerdings nicht automatisch, sondern bedarf einer Prüfung im Einzelfall, die im Folgenden weiter ausgeführt wird.

Mangels entsprechender gesetzlicher Vorgaben im De-Mail-Gesetz sind nicht die DMDA, sondern die Versender von De-Mails für die Beachtung datenschutzrechtlich angemessener Verfahren verantwortlich. Um ein angemessenes Schutzniveau bei der Versendung besonders schutzbedürftiger personenbezogener Daten (z.B. Sozialdaten oder Daten die Rückschlüsse auf den Gesundheitszustand einzelner Betroffener zulassen) mittels De-Mail zu gewährleisten, ist aus datenschutzrechtlicher Sicht eine Ende-zu-Ende-Verschlüsselung grundsätzlich erforderlich. Die Vorgaben des De-Mail-Gesetzes, die Technische Richtlinie des BSI nach § 18 Abs. 2 De-Mail-Gesetz und der Kriterienkatalog des BfDI gemäß § 18 Abs. 3 Nr. 4 De-Mail-Gesetz machen zwar deutlich, dass bei De-Mail das Datenschutz- und Datensicherheitsniveau im Vergleich zum E-Mail-Versand erheblich höher ist. Trotzdem müssen über diesen Mindeststandard hinaus beim Versand besonders schutzbedürftiger Daten grundsätzlich zusätzliche Schutzvorkehrungen getroffen werden.

Ob eine Ende-zu-Ende-Verschlüsselung im Einzelfall die datenschutzrechtlich angemessene Sicherungsmaßnahme darstellt, orientiert sich an dem konkreten Schutzbedarf der Daten. Dieser ist zunächst anhand der Grundschutzmethodik des BSI von der datenverarbeitenden Stelle festzustellen:

- Bei einer Schutzbedarfsfeststellung ist grundsätzlich danach zu fragen, welcher Schaden entstehen kann, wenn die Grundwerte Vertraulichkeit, Integrität oder Verfügbarkeit verletzt werden. Es muss also gefragt werden, welcher Schaden eintritt, wenn vertrauliche Informationen unberechtigt zur Kenntnis genommen oder weitergegeben werden (Verletzung der Vertraulichkeit), die Korrektheit der Informationen und die Funktionsweise von Systemen nicht mehr gegeben ist (Verletzung der Integrität) oder autorisierte Benutzer am Zugriff auf Informationen und Systeme behindert werden (Verletzung der Verfügbarkeit). Dabei wird zwischen den Schutzbedarfskategorien „normal“, „hoch“ und „sehr hoch“ unterschieden. Der Schaden, der von einer Verletzung der Grundwerte ausgehen kann, kann sich auf verschiedene Schadensszenarien beziehen:
    - Verstöße gegen Gesetze, Vorschriften oder Verträge,
    - Beeinträchtigungen des informationellen Selbstbestimmungsrechts,
    - Beeinträchtigungen der persönlichen Unversehrtheit,
    - Beeinträchtigungen der Aufgabenerfüllung,
    - negative Außenwirkung oder
    - finanzielle Auswirkungen.

- Beim Schutzbedarf „normal“ sind die Schadensauswirkungen begrenzt und überschaubar. Beim Versand von Daten mit dem Schutzbedarf „normal“ ist eine Ende-zu-Ende-Verschlüsselung dann nicht notwendig.

- Beim Schutzbedarf „hoch“ können die Schadensauswirkungen beträchtlich sein. Beim Versand von Daten mit dem Schutzbedarf „hoch“ ist eine Ende-zu-Ende-Verschlüsselung grundsätzlich erforderlich. Auf sie kann jedoch dann verzichtet werden, wenn die datenverarbeitende Stelle anhand einer Risikoanalyse zu dem Ergebnis kommt, dass sie aufgrund der getroffenen technischen und organisatorischen Sicherheitsmaßnahmen das Restrisiko im Bereich des Versenders als vertretbar bewertet. Versender und Empfänger müssen sich aber auf jeden Fall an ihrem Konto im Sinne des § 4 Abs. 1 Satz 2 De-Mail-Gesetz sicher anmelden.

- Beim Schutzbedarf „sehr hoch“ können die Schadensauswirkungen bei unberechtigtem Zugriff ein existentiell bedrohliches Ausmaß erreichen. Beim Versand von Daten mit dem Schutzbedarf „sehr hoch“ ist eine Ende-zu-Ende-Verschlüsselung zwingend notwendig.

- Bei der Schutzbedarfsanalyse ist Folgendes zu beachten:

    - Die Einstufung des jeweiligen personenbezogenen Datums kann je nach Kontext, in dem das Datum verwendet wird, unterschiedlich sein. So ist beispielsweise der Schutzbedarf einer Adresse im Regelfall behördlicher Anwendungen normal oder hoch. Befindet sich die betroffene Person aber in einem Zeugenschutzprogramm, ist der Schutzbedarf sehr hoch und die Daten dürften nur mit Ende-zu-Ende-Verschlüsselung übertragen werden.

    - Sozial- und Steuergeheimnisdaten sind zwar nach dem Gesetz insofern als besonders schützenswert eingestuft, als ihre Verarbeitung zum Teil besonderen Restriktionen unterliegt. Allerdings bedeutet dies nicht, dass sämtliche Sozial- und Steuergeheimnisdaten Ende-zu-Ende-verschlüsselt werden müssen. Die Tatsache, dass eine Person beispielsweise bei einer bestimmten gesetzlichen Krankenkasse versichert ist, ist im Regelfall kein besonders schützenswertes Datum.

    - Gesundheitsdaten unterliegen dagegen in aller Regel dem Schutzbedarf „sehr hoch“. Dies gilt wiederum auch unabhängig vom Kontext als Sozialdatum. Auch die Angabe von besonderen Belastungen bei

Krankheitsaufwendungen im Zusammenhang mit einer Einkommenssteuererklärung sind besonders schutzbedürftig, auch wenn Steuergeheimnisdaten nicht automatisch Ende-zu-Ende-verschlüsselt werden müssen.

Neben der Schutzbedarfsanalyse muss für eine Einschätzung der notwendigen Sicherheitsmaßnahmen beim Versand besonders schutzbedürftiger Daten auch berücksichtigt werden, wer Versender und Empfänger der De-Mail ist:

- Versenden Behörden oder andere Institutionen besonders schutzbedürftige personenbezogene Daten unmittelbar an den Betroffenen, richtet sich die Verpflichtung zur Ende-zu-Ende-Verschlüsselung grundsätzlich nach dem im Wege der Schutzbedarfsanalyse ermittelten Schutzbedarf der Daten. Daneben muss der Versender vor dem Versand das Einverständnis des potentiellen Empfängers einholen[1]. Dies sollte mindestens einmalig für alle diesen Transportweg betreffenden Kommunikationsvorgänge erfolgen. Zusätzlich muss für den Versand besonders schutzbedürftiger Daten mittels De-Mail an den Betroffenen eine individuelle Zugangseröffnung vorliegen[2]. Dies gilt insbesondere für eine differenzierte Betrachtung bei der Zugangseröffnung gegenüber Behörden. Der Bürger sollte die Möglichkeit haben, den Zugang differenziert nach einzelnen Behörden zu gestalten.

- Versenden Behörden oder andere Institutionen wie etwa gesetzliche Krankenkassen, die mit besonders schutzbedürftigen personenbezogenen Daten Dritter umgehen, solche Daten untereinander, muss die Nachricht im Ergebnis auch ohne ein Schutzbedarfsanalyse Ende-zu-Ende verschlüsselt werden. Betrachtet man den Versand einzelner Nachrichten, würde eine Schutzbedarfsanalyse an sich zu dem Ergebnis kommen, dass in bestimmten Fällen (z.B. beim Schutzbedarf „normal“) eine Ende-zu-Ende-Verschlüsselung nicht erforderlich ist. Hier muss aber berücksichtigt werden, dass im Falle eines unberechtigten Zugriffs beim DMDA durch die Vielzahl der versandten bzw. empfangenen Daten ein erhöhtes Angriffsrisiko und Schadenspotential vorliegt (Kumulationseffekt). Außerdem kann der Betroffene nicht entscheiden, auf welche Weise seine Daten versandt werden. Die Tatsache, dass der Betroffene in diesen Fällen keinen Einfluss auf die Ausgestaltung der De-Mail-Nutzung nehmen kann, darf nicht zu einer Absenkung des Datenschutzniveaus bei der Versendung

[1] Dies gilt generell für den Versand personenbezogener Daten, also auch für solche, die als nicht besonders schutzbedürftig eingestuft werden.
[2] Vgl. Fußnote 1.

besonders schutzbedürftiger Daten mittels De-Mail führen. Schließlich kann man davon ausgehen, dass solche Einrichtungen den De-Mail-Dienst über ein Gateway nutzen können und daher eine Ende-zu-Ende-Verschlüsselung in diesen Fällen mit vertretbarem technischen Aufwand möglich ist. Die Verpflichtung gilt unabhängig von der Größe der Einrichtung und unabhängig davon, ob eine gesetzliche Pflicht zur Datenverarbeitung besteht. Letztlich führt die einheitliche Behandlung alle Nachrichteninhalte in diesem Kommunikationsverhältnis auch zur einer handhabbaren Anwendung für Versender und Empfänger.

Der Entwicklungsstand der Technik und die tatsächliche Verfahrensweise im Umgang mit De-Mail muss beobachtet werden. Daraus können sich in Zukunft neue oder andere Anforderungen des Datenschutzes an die Verwendung von De-Mail und die Verschlüsselung ergeben. Die DMDA werden aufgefordert, leicht handhabbare Verschlüsselungsoptionen für die Nutzer zu entwickeln. Dies kann auch Datenschutzverstöße aufgrund einer fehlerhaften Schutzbedarfsfeststellung der verantwortlichen Stelle verhindern.

Schließlich müssen auch die internen Verfahrensabläufe bei der versendenden sowie bei der empfangenden Stelle betrachtet werden, also z.B. die Verknüpfung des Fachverfahrens mit dem De-Mail-Postfach und interne Zugriffsberechtigungen in den Unternehmen und Behörden. Auch diese müssen datenschutzkonform ausgestaltet sein und die Sicherheit der Daten gewährleisten.