Technische Richtlinie Sicherer E-Mail-Transport

Florian Bierhoff · Thomas Gilles

Bundesamt für Sicherheit in der Informationstechnik
{florian.bierhoff | thomas.gilles}@bsi.bund.de

Zusammenfassung

Die Technische Richtlinie BSI TR-03108 Secure E-Mail Transport adressiert die Transportsicherheit von E-Mails und zeigt einen Lösungsansatz, wie die Anzahl an sicher versendeten E-Mails ohne Mehraufwand für den Nutzer erhöht werden kann. Ein Großteil unserer digitalen Kommunikation findet heute via E-Mail statt, wobei nachweislich die konsequente Anwendung von IT-Sicherheitsmaßnahmen häufig vernachlässigt wird. Um dem entgegen zu wirken wurde ein einheitlicher Standard definiert, der den E-Mail-Diensteanbietern als Blaupause für den sicheren Betrieb ihres E-Mail-Dienstes dient. Dabei zielen die Maßnahmen insbesondere auf die funktional und kryptografisch sichere Konfiguration der Kommunikationsschnittstellen ab, um eine hochwertige Transportsicherheit zu gewährleisten. Ferner wird über den Standard die Vergleichbarkeit der Sicherheit von E-Mail-Diensteanbietern möglich. Dabei wurde bewusst auf etablierte IT-Sicherheitsstandards aufgesetzt und darauf geachtet, dass die Umsetzung der Anforderungen alleine durch den E-Mail-Diensteanbieter erfolgen kann. Ein in sich geschlossenes Netzwerk oder die Verlagerung der IT-Sicherheitsmaßnahmen zu Sender und Empfänger der E-Mail wurden aus verschiedenen Gründen im Laufe des Vorhabens nicht weiter verfolgt. Das Ergebnis ist ein übersichtliches Regelwerk, welches modular aufgebaut ist und dessen Wirkung nicht alleine von einer hundertprozentigen Umsetzung in der Praxis abhängt.

1 Einführung

In unserer digitalen Kommunikation spielt die E-Mail nach wie vor eine wichtige Rolle. Häufig sind Sender und Empfänger von E-Mails sich nicht bewusst, dass E-Mails nicht zwangsläufig unter der Anwendung ausreichender IT-Sicherheitsmaßnahmen, wie Verschlüsselung und Signatur, transportiert werden. Ähnlich einer Postkarte können ungeschützte E-Mails von jeder Stelle, über die sie weitergeleitet werden, mitgelesen, manipuliert oder zu anderen Stellen umgeleitet werden.

Hauptgrund für diesen Effekt ist, dass für den Sender und den Empfänger die grundsätzliche Funktionstüchtigkeit des E-Mail-Transports bzw. die erfolgreiche Zustellung der E-Mail im Vordergrund steht. Weitere Ziele, wie Vertraulichkeit und Integrität, werden als zweitrangig bzw. entbehrlich betrachtet. Auch Ende-zu-Ende-Sicherheit findet, trotz der mittlerweile guten Verfügbarkeit entsprechender Software und Infrastrukturen, keine breite Anwendung. Hier werden vor allem die Verwaltung der privaten und öffentlichen Schlüssel sowie die Verifikation der jeweiligen Kommunikationspartner als zu komplex betrachtet.

Eine Ende des Jahres 2015 von Google veröffentlichte Studie [DAM+15] kommt zu dem Ergebnis, dass zwar der Anteil der E-Mails, die sicher übertragen werden, insgesamt in den vergangenen Jahren gestiegen ist. Jedoch wurden von den Gmail Servern Ende 2015 noch immer

P. Schartner (Hrsg.) · D•A•CH Security 2016 · syssec (2016) 321-327.

40% der eingehenden und 20% der ausgehenden E-Mails ohne die Anwendung von IT-Sicherheitsmaßnahmen verschickt, weil die jeweilige Gegenseite die entsprechenden Funktionalitäten nicht unterstützte.

1.1 Ziele und Anforderungen

Primäres Ziel des Vorhabens ist es, die Anzahl der auf sichere Art und Weise zwischen E-Mail-Diensteanbietern sowie Sendern und Empfängern ausgetauschten E-Mails zu erhöhen. Dieses Ziel soll erreicht werden, ohne dass für Sender und Empfänger zusätzliche Aufwände entstehen. Gleichzeitig sollen die E-Mail-Diensteanbieter durch die Nutzung der Technischen Richtlinie als Arbeitsgrundlage mehr Planungssicherheit erhalten und im Rahmen eines Zertifizierungsverfahrens die Einhaltung der Anforderungen an einen sicheren E-Mail-Transport überprüfen und gegenüber Dritten nachweisen können.

Durch die Betrachtung aller Kommunikationsbeziehungen innerhalb der E-Mail-Infrastruktur wird mit der Technischen Richtlinie die Strecke vom Sender zum Empfänger einer E-Mail vollständig von Punkt-zu-Punkt betrachtet, ohne dass der Aufbau einer neuen Infrastruktur notwendig wird.

1.2 Herangehensweise

Schon zu Beginn der Konzeptionsphase wurden die ersten Überlegungen gemeinsam mit bereits am Markt tätigen E-Mail-Diensteanbietern diskutiert. Das dabei zunächst angedachte Konzept einer geschlossenen Gruppe von vertrauenswürdigen E-Mail-Diensteanbietern wurde jedoch relativ schnell wieder verworfen, da dies nur einen mehr oder weniger großen Zirkel in der gesamten E-Mail-Infrastruktur erreicht hätte. Ein weiterer Grund für diese Entscheidung ist die Tatsache, dass die E-Mail-Diensteanbieter, welche sich an die Vorgaben der Technischen Richtlinie halten, auch in Zukunft mit solchen E-Mail-Diensteanbietern kommunizieren werden, die dies nicht tun. Stattdessen wurde daher schon zu Beginn des Projekts entschieden die grundsätzliche Offenheit der global verteilten E-Mail-Infrastruktur zu berücksichtigen und auf Technologien zu setzen, die auch dann ihre Wirkung entfalten, wenn einer oder beide Kommunikationspartner nur bestimmte Teile der Technischen Richtlinie unterstützen.

Dieses Konzept wurde anschließend im Zuge der Veröffentlichung eines ersten Entwurfs der Technischen Richtlinie in die neu vom Bundesamt für Sicherheit in der Informationstechnik (BSI) gegründete Arbeitsgruppe zur Finalisierung und Fortschreibung der Technischen Richtlinie eingebracht. Dort und auch in der Fachpresse stieß das Konzept auf sehr positives Interesse, weshalb es anschließend gemeinsam mit über 20 in der Arbeitsgruppe mitarbeitenden E-Mail-Diensteanbietern weiter präzisiert und schließlich finalisiert werden konnte.

Ebenfalls in dieser Phase eingebunden wurden verschiedene internationale Partner des BSI sowie Verbände, denen die Möglichkeit gegeben wurde sich in die Finalisierung der Technischen Richtlinie einzubringen. Mittlerweile wurde die finale Version der Technischen Richtlinie veröffentlicht und findet unter den Beteiligten große Akzeptanz.

2 Lösungsansatz

Der Lösungsansatz wurde in engem Dialog mit verschiedenen am Markt tätigen E-Mail-Diensteanbietern erarbeitet und zeichnet sich durch die konsequente Verwendung etablierter

(z.B. TLS) und innovativer Technologien (z.B. DANE) aus. Neben der Verwendung frei verfügbarer offener Standards ist bei der Erstellung der Technischen Richtlinie darauf geachtet worden, dass diese in einer offenen Infrastruktur eingesetzt wird und sich positive Effekte auch dann einstellen, wenn sich nicht alle Teilnehmer der E-Mail-Infrastruktur an die Vorgaben der Technischen Richtlinie halten. So wirkt sich zum Beispiel die Verwendung von sicherer Kryptographie auch dann positiv auf die Sicherheit der Kommunikationsverbindung aus, wenn sie nicht durch gesicherte DNS-Abfragen und obligatorische Verschlüsselung unterstützt wird. Unabhängig von der Umsetzung der in der Technischen Richtlinie geforderten Technologien, können die öffentlichen kryptografischen Schlüssel auch über andere Wege bereitgestellt und überprüfbar gemacht werden. Auch ist in die Erarbeitung des Lösungsansatzes eingeflossen, dass den Nutzern der E-Mail-Dienstleistung kein zusätzlicher Aufwand durch die Etablierung der Technischen Richtlinie entsteht.

Erleichtert wird die Umsetzung der Technischen Richtlinie dadurch, dass diese modular aufgebaut ist und die verschiedenen Bausteine eines sicheren E-Mail-Dienstes nach und nach von den E-Mail-Diensteanbietern umgesetzt werden können. Durch die konsequente Verwendung von vorhandenen Standards, können die E-Mail-Diensteanbieter an vielen Stellen auf Maßnahmen aufbauen, die bereits in den eigenen Systemen umgesetzt wurden, aber z.B. noch nicht optimal konfiguriert sind. Beispielhaft gilt dies zum Beispiel für die Wahl passender kryptografischer Algorithmen und Verbindungsparameter. Viele E-Mail-Dienste bieten zwar schon kryptographisch gesicherte Verbindungen an, setzen jedoch auf veraltete und/oder mittlerweile als unsicher geltende Algorithmen. Hier kann durch die Konfiguration der Bevorzugung zeitgemäßer Kryptographie bei einer Kommunikation die Sicherheit entscheidend erhöht werden.

Insgesamt wird jeder E-Mail-Diensteanbieter, der die Maßnahmen umsetzt, zu einem Baustein in einer sicheren Transport-Infrastruktur von der alle Teilnehmer profitieren.

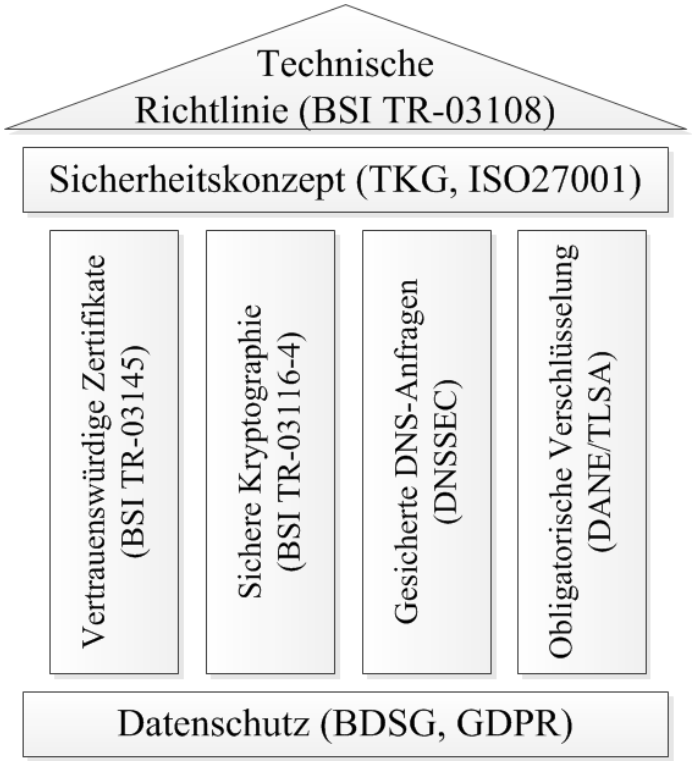

Abb. 1: Konzeptionelle Übersicht

Die vorstehende Abbildung verdeutlicht den modularen Aufbau der Technischen Richtlinie, indem die einzelnen Maßnahmen als Säulen einer Gesamtkonstruktion dargestellt werden. Erst durch die vollständige Umsetzung der einzelnen Maßnahmen ergibt sich ein einheitliches Sicherheitsniveau.

Das Zusammenwirken der einzelnen Maßnahmen und deren Bedeutung werden in den folgenden Unterkapiteln erläutert.

2.1 Sicherheitskonzept

Grundlage für eine Aussage über die Vertrauenswürdigkeit eines E-Mail-Diensteanbieters ist, dass dieser ein Sicherheitskonzept für den bei ihm betriebenen E-Mail-Dienst vorweisen kann. In Deutschland tätige E-Mail-Diensteanbieter können hier auf ein anhand der Anforderungen des Telekommunikationsgesetzes erstelltes Sicherheitskonzept oder im internationalen Bereich auf ein ISMS, welches anhand des international anerkannten Standards ISO/IEC 27001 erstellt worden ist, zurückgreifen. Die Erstellung und Umsetzung eines Sicherheitskonzeptes bildet die Grundlage für den sicheren Betrieb. Hierdurch können viele externe und interne Angriffe auf die Systeme des E-Mail-Diensteanbieters bereits im Vorfeld systematisch verhindert werden. Das Sicherheitskonzept muss jedoch nicht nur die Sicherheit zu einem bestimmten Zeitpunkt betrachten, sondern muss kontinuierlich gelebt und fortgeschrieben werden. Gerade diesen Bereich adressiert die Zertifizierung nach ISO/IEC 27001.

2.2 Vertrauenswürdige Zertifikate

Einer der etablierten Vertrauensanker im digitalen Handeln sind Zertifizierungsstellen, welche die Authentizität von Zertifikaten bestätigen. Die Zertifikate beinhalten in diesem Fall von der Zertifizierungsstelle geprüfte Informationen zum Inhaber des Zertifikats selbst (z.B. Organisationsname) aber auch kryptographische Informationen. Insbesondere der öffentliche Schlüssel und damit auch ein vertrauenswürdiger Verweis auf den privaten Schlüssel, werden von der Zertifizierungsstelle bestätigt. Darüber hinaus werden von der Zertifizierungsstelle durch eine sogenannte Certificate Policy die Bedingungen zur Erstellung, zum Umgang und zur Nutzung der Zertifikate festgeschrieben, an welche die Teilnehmer gebunden sind. Die Technische Richtlinie referenziert Anforderungen an eine vertrauenswürdige Zertifizierungsstelle, die den E-Mail Diensteanbieter bei seiner Auswahl unterstützen sollen.

Die Nutzung vertrauenswürdiger Zertifikate dient vor allem dem Zweck, dass ausschließlich authentische kryptographische Schlüssel eingesetzt werden. So kann verhindert werden, dass Angreifer durch Man-in-the-Middle-Attacken die verschlüsselte Kommunikation unterlaufen.

Vertrauenswürdige Zertifikate erlauben es unabhängig von einem automatisierten Mechanismus zum Austausch von Zertifikaten, die Authentizität einer elektronischen Identität nachzuweisen. Sie werden daher trotz der, in der Technischen Richtlinie verankerten, verpflichtenden Anforderung nach dem Einsatz von DNSSEC und DANE/TLS, gefordert, um auch mit Teilnehmern der E-Mail-Infrastruktur, die noch nicht DNSSEC und DANE/TLSA unterstützen, überprüfbar sichere Verbindungen aufzubauen. Überdies verfügen die Zertifizierungsstellen über einen Sperrmechanismus für nicht mehr vertrauenswürdige Zertifikate.

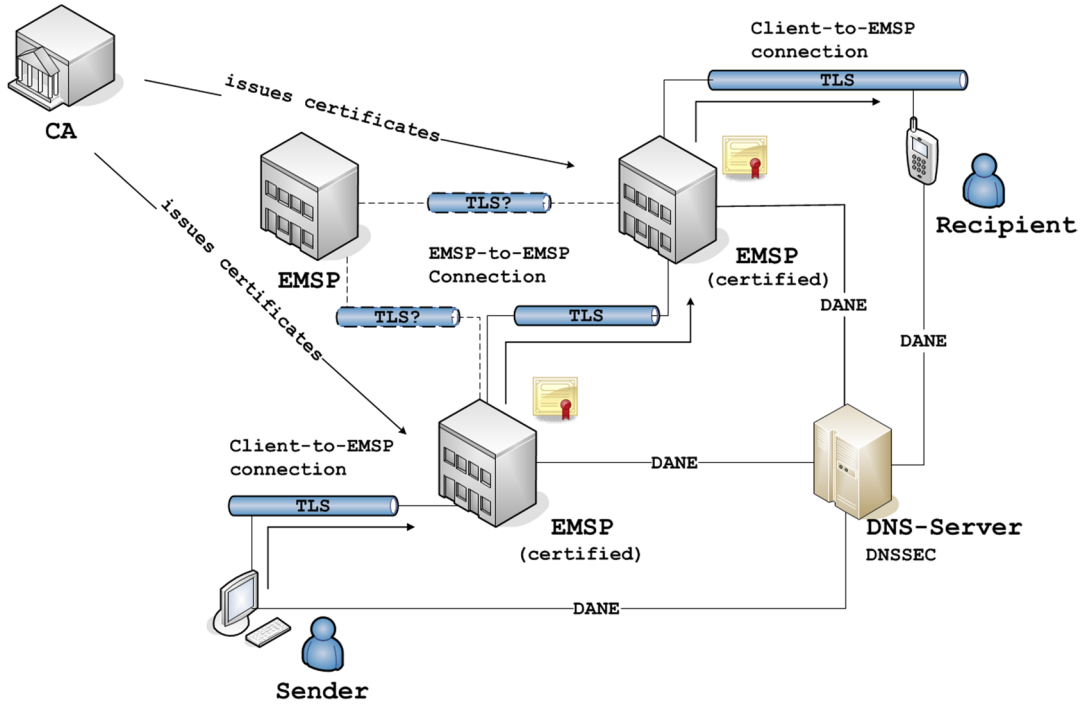

Abb. 2: Infrastrukturübersicht

Die vorstehende Abbildung verdeutlicht die Rolle, welche den Zertifizierungsstellen (CAs) in der Gesamtinfrastruktur zukommt. Auch wird in durch die Abbildung deutlich, dass die Forderung nach vertrauenswürdigen Zertifikaten (CAs) und nach obligatorischer Verschlüsselung (DNSSEC und DANE/TLSA) sich ergänzende Anforderungen darstellen, welche die E-Mail-Infrastruktur insgesamt sicherer machen.

2.3 Sichere Kryptographie

Um die Kommunikation zwischen den E-Mail-Diensteanbietern untereinander und auch zu dem Nutzer hin zu schützen, werden diese kryptographisch abgesichert. Schon jetzt werden viele Kommunikationsverbindungen im Internet auf diese Weise gesichert, jedoch ist leider auch die Übertragung im Klartext keine Seltenheit. Dies passiert insbesondere dann, wenn die eingesetzten kryptographischen Verfahren der Kommunikationspartner inkompatibel sind oder es beim Verbindungsaufbau zu Fehlern kommt. Nicht selten werden aus Gründen der Abwärtskompatibilität auch Verfahren eingesetzt, die mittlerweile keine ausreichende Sicherheit mehr für den Inhalt der zu transportierenden Daten bieten.

Die Technische Richtlinie fordert daher ein Mindestmaß an Algorithmen, die von den E-Mail-Diensteanbietern umgesetzt werden müssen. Dabei wird in der Technischen Richtlinie auf die Technische Richtlinie „Kryptographische Vorgaben für Projekte der Bundesregierung“ [BSI16] verwiesen. Letztere wird vom BSI jährlich und anlassbezogen aktualisiert und stellt bei Einhaltung sicher, dass zeitgemäße Kryptographie eingesetzt wird.

Hierdurch soll unterbunden werden, dass Algorithmen verwendet werden, die nicht mehr als sicher eingestuft werden. Gemäß der Technischen Richtlinie für den sicheren E-Mail-Transport müssen die in der oben genannten Technischen Richtlinie für Kryptographie spezifizierten Algorithmen bevorzugt angeboten werden. Letzten Endes lässt sich, auch wenn der einzelne E-Mail-Diensteanbieter sich an die Vorgaben der Technischen Richtlinie hält, auch in Zukunft

nicht ausschließen, dass unzureichend abgesicherte Verbindungen mit Kommunikationspartnern aufgebaut werden, die sich ihrerseits nicht an die Vorgaben der Technischen Richtlinie halten. Durch die Umsetzung der Vorgaben der Technischen Richtlinie ist der E-Mail-Diensteanbieter aber für eine sichere Kommunikation vorbereitet und entsprechend sollen sichere Verbindungen zur Regel werden.

2.4 Gesicherte DNS-Anfragen durch DNSSEC

Die sogenannten DNS-Server sind eine der wichtigsten Infrastruktur-Komponenten im Internet, da durch Sie die menschen-verständlichen Adressen, welche im Browser und anderer Software genutzt werden, in logische Adressen umgewandelt werden. Ihnen kommt auch deswegen eine besonders wichtige Aufgabe zu, weil eine Manipulation der Kommunikation mit dem DNS-Server ein Umlenken auf eine andere Zieladresse erlaubt. Um solche Manipulationen vorzubeugen wurden weltweit geltende Vorgaben zur Signierung von DNS-Antworten von der Internet Assigned Numbers Authority (IANA) definiert, die auf dem Einsatz des internationalen Standards DNSSEC nach [KoMG12] basieren. Sichere DNS-Abfragen sind eine Grundvoraussetzung, um sicherzustellen, dass in der späteren Kommunikation mit dem E-Mail-Diensteanbieter die korrekte Gegenstelle adressiert wird.

Da die DNS-Server auch für die Einleitung der in dem folgenden Kapitel beschriebenen obligatorischen Verschlüsselung verantwortlich sind, kommt Ihnen in diesem Szenario eine besonders wichtige Rolle zu. Eine Manipulation der DNS-Anfragen und natürlich insbesondere der –Antworten könnte es einem Angreifer erlauben die spätere Verschlüsselung zu unterwandern. Dies wird durch den konsequenten Einsatz von DNSSEC unterbunden.

2.5 Obligatorische Verschlüsselung mittels DANE

Um den Mehrwert, den diese Technische Richtlinie bieten soll, zu entfalten ist es wichtig, dass die bisher beschriebenen Sicherheitsmaßnahmen auch durchgesetzt werden. Die mittlerweile auch in der Praxis erprobte Technologie DANE nach [HoSc12] erfüllt in diesem Kontext gleich zwei wichtige Funktionen. Zum einen stellt der Einsatz von DANE und die damit verbundene Erweiterung des DNS-Records ein Statement für diejenigen, die mit einer Internetadresse kommunizieren möchten, dar, dass der Zielserver kryptographische Protokolle unterstützt und entsprechend verschlüsselt kommunizieren möchte. Zum anderen können mit Hilfe von DANE auch Informationen zum Zertifikat selbst (z.B. Hashwert über das Zertifikat) bereitgestellt werden, die eine einfache Möglichkeit zur Verifikation der Echtheit bieten. Durch die Kombination mit den im vorherigen Kapitel beschriebenen sicheren DNS-Abfragen werden auch Angriffe, wie das Unterdrücken des Befehls zu Initialisierung einer sicheren Verbindung mit dem E-Mail-Server (STARTTLS) abgewandt, da eine Manipulation des DNS-Records und kryptographischen Materials verhindert wird. Letztlich wird ein E-Mail-Diensteanbieter, gemäß der Technischen Richtlinie, mit einem Kommunikationspartner der DANE einsetzt, ausschließlich verschlüsselt kommunizieren.

2.6 Datenschutz

Neben der sicheren Verwendung von IT-Technologie zur Datensicherheit, müssen auch hohe Anforderungen an den Datenschutz gestellt werden. Die IT-Sicherheit darf nicht durch unberechtigte interne Vorgänge unterwandert werden, so dass sensible Informationen an Dritte geraten. Um diesem Anspruch gerecht zu werden, bezieht sich die Technische Richtlinie konkret

auf Unternehmen, die künftig an die Einhaltung der EU-weit geltenden Datenschutz-Grundverordnung und deren nationalen Umsetzungen gebunden sind. In Deutschland z.B. sind die E-Mail-Diensteanbieter an das Bundesdatenschutzgesetz gebunden.

3 Zusammenfassung und Ausblick

Die Technische Richtlinie dient nicht dazu eine geschlossene hochsichere Infrastruktur zu schaffen, sondern versucht durch die Kombination bestehender Standards eine gemeinsame Basis an IT-Sicherheit innerhalb der grundsätzlich offenen E-Mail-Infrastruktur zu etablieren. Auf diese Weise soll die sichere E-Mail-Kommunikation deutlich gesteigert werden. Die Transparenz für den Nutzer wird dadurch erhöht, das E-Mail-Diensteanbieter sich bewusst an die Vorgaben der Technischen Richtlinie halten und dies kommunizieren.

Einen besonderen Mehrwert bietet in diesem Zusammenhang ein derzeit im Aufbau befindliches Zertifizierungsverfahren. Durch dieses wird der E-Mail-Diensteanbieter zusätzlich in die Lage versetzt, die Einhaltung der Vorgaben der Technischen Richtlinie durch einen Dritten prüfen zu lassen und somit seinen Nutzern und anderen gegenüber einen belastbaren Sicherheitsnachweis zu erbringen.

Auch denjenigen E-Mail-Diensteanbietern, die sich gegen eine Zertifizierung entscheiden, dient die Technische Richtlinie als wichtige Leitlinie, wenn es um die Auswahl von sicherheitsrelevanten Funktionen und deren Konfiguration (z.B. Algorithmen und Protokolle) geht.

Durch die große Resonanz und umfangreiche Beteiligung von E-Mail-Diensteanbietern in der Arbeitsgruppe, ist bereits ein Großteil des privaten E-Mail-Aufkommens in Deutschland adressiert. Die Technische Richtlinie spricht aber auch schon jetzt Unternehmen an, bei denen der E-Mail-Dienst kein Geschäftsszenario, aber eine wichtige Infrastruktur zur internen und externen Kommunikation darstellt. Schon jetzt wurde an das BSI ein Interesse zur Umsetzung der Technischen Richtlinie aus verschiedensten Branchen (z.B. Versicherungsgesellschaften) und dem universitären Umfeld herangetragen.

Sollte das aktuelle Interesse auch in eine praktische Umsetzung münden, wird durch die Technische Richtlinie viel zur Erhöhung der IT-Sicherheit bei privater sowie geschäftlicher Kommunikation beigetragen und potenziellen Angreifern das Leben erschwert.

Literatur

[DAM+15] Z. Durumeric, D. Adrian, A. Mirian, J. Kasten, E. Bursztein, N. Lidzborski, K. Thomas, V. Eranti, M. Bailey, J. A. Halderman: Neither Snow Nor Rain Nor MITM... An Empirical Analysis of Email Delivery Security, In Proceedings of Internet Measurement Conference (IMC), 2015.

[BSI16] Bundesamt für Sicherheit in der Informationstechnik: BSI TR-03116 Kryptographische Vorgaben für Projekte der Bundesregierung Teil 4 – Kommunikationsverfahren in Anwendungen, 2016.

[KoMG12] O. Kolkman, W. Mekking, R. Gieben: DNSSEC Operational Practices, Version 2, RFC 6781, 12/2012.

[HoSC12] P. Hoffman, J. Schlyter: The DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA, RFC 6698, 08/2012.