ersichtlich geworden, dass gerade bei den zustandsbehafteten hashbasierten Signaturverfahren gewisse Einschränkungen im Hinblick auf die gewünschten Kriterien gelten, die sorgfältig berücksichtigt werden müssen.

Letztlich wurden weitere Schritte wie die Zertifikatsgestaltung sowie das Migrationskonzept erläutert. Es steht fest, dass die Migration hochkomplexer PKI wie die Verwaltungs-PKI enorm aufwendig und langwierig ist. Daher ist es wichtig, die Migration frühzeitig zu planen und einzuleiten, um den Umstieg zur Post-Quanten-Kryptografie rechtzeitig und mit der erforderlichen Betriebskontinuität umsetzen zu können.

Sichere E-Mail-Kommunikation

Technische Richtlinien „Secure Email Transport“ und „Email Authentication“

Die E-Mail ist nach wie vor eines der wichtigsten Kommunikationsmittel. Obwohl Vertraulichkeit und Integrität der Nachrichten in vielen Fällen schützenswert sind, werden E-Mails häufig ungesichert ohne Signatur und Verschlüsselung versendet.

Von Kristina Pohl und Thomas Gilles, Cyber-Sicherheit in Smart Home und Smart Cities

Eine sichere E-Mail-Kommunikation ist für den beruflichen sowie privaten Alltag vieler Bürgerinnen und Bürger von großer Bedeutung. Darum engagiert sich das BSI in diesem Bereich auf nationaler und internationaler Ebene mit dem Ziel, die Vertrauenswürdigkeit und Sicherheit in die E-Mail-Kommunikation nachhaltig zu stärken. Diese Aufgabe stellt eine große Herausforderung dar, denn bei der Entwicklung der E-Mail blieb der Sicherheitsaspekt noch unbeachtet. Die Sicherheitsverfahren zum Schutz der Kommunikation wurden erst im Nachgang als Ergänzungen konzipiert. Weitere Gründe sind vor allem die große Anzahl heterogener Kommunikationsteilnehmer und deren unterschiedliche Systeme. Dies gilt sowohl in Bezug auf die Nutzerinnen und Nutzer als auch auf die E-Mail-Diensteanbieter (EMDA). Die Nutzerinnen und Nutzer haben unterschiedliche Sicherheitsbedürfnisse, und nur wenige beschäftigen sich mit den Risiken und den dazu passenden Lösungen. Überdies existieren verschiedene Sicherheitsverfahren, die von den EMDA eingesetzt werden können. Zudem müssen die Maßnahmen bei den miteinander kommunizierenden EMDA aufeinander abgestimmt sein, um ihre volle Wirksamkeit entfalten zu können und Inkompatibilitäten zu vermeiden.

Als einheitliche Leitlinie dienen dafür die Technischen Richtlinien des BSI. Sie sind eine wichtige Orientierungsgrundlage, denn sie beschreiben, welche Verfahren aktuell am besten geeignet sind, um die Sicherheit im Bereich E-Mail signifikant und zukunftssicher zu erhöhen. Zudem geben die Richtlinien Hinweise („Best Practices“) für eine korrekte Implementierung und sinnvolle Konfiguration, um Fehler bei der Umsetzung der Maßnahmen schon von Beginn an zu vermeiden.

In den Technischen Richtlinien „Sicherer E-Mail-Transport“ (BSI TR-03108) und „Authentische E-Mail“ (BSI TR-03182) werden Maßnahmen beschrieben, mit denen E-Mail-Diensteanbieter das Sicherheitsniveau – ohne zusätzlichen Aufwand für die Nutzerinnen und Nutzer – deutlich verbessern können.

Praxisnahe Standards

Um dem Stand der Technik fortlaufend gerecht zu werden, wurde am 1. Juni 2023 die aktualisierte und erweiterte Version 2.0 der TR-03108 veröffentlicht. Die Version 2.0 basiert auf bereits am Markt etablierten sowie zukunftsträchtigen Sicherheitsstandards. Zugleich wurden die Vorgaben für Kryptoalgorithmen aktualisiert. Diese müssen zukünftig immer den Anforderungen aus der aktuellsten Version der BSI TR-03116-4 „Kryptographische Vorgaben für Projekte der Bundesregierung“ entsprechen. Neu ist auch die Forderung nach einem Reporting-Mechanismus, dem SMTP TLS Reporting (TLS RPT). Es handelt sich dabei um das einzige in der TR-03108 geforderte Verfahren, das bisher wenig Verbreitung gefunden hat. Das BSI hat TLS RPT als neu gefordertes Verfahren in die TR eingeführt, weil dieses Verfahren einen Rückkanal von EMDA zu EMDA bietet und somit die anderen geforderten Sicherheitsmechanismen aus der TR ergänzt. Durch das automatische Reporting können technische Probleme und Sicherheitsrisiken erkannt und beseitigt werden. Ein emp-

fangender EMDA kann mit TLS RPT an den sendenden EMDA einer E-Mail automatisiert zurückmelden, ob eine gesicherte Kommunikation erfolgreich durchgeführt werden konnte.

Sicher verschlüsseln – so gehts

EMDA ermöglichen durch die Nutzung von Transport Layer Security (TLS) jedem Kommunikationspartner die Zustellung verschlüsselter E-Mails. Aufgrund der heterogenen Systeme der EMDA, die in die E-Mail-Kommunikation involviert sind, kann die zu verwendende TLS-Version vor dem Verbindungsaufbau jedoch nicht strikt vorgegeben werden. Denn vor dem Beginn der Kommunikation steht nicht fest, welcher EMDA jeweils welche TLS-Version unterstützt. Das von der Internet Engineering Task Force (IETF) standardisierte Protokoll DNS-based Authentication of Named Entities (DANE) ermöglicht bereits vor dem Beginn der eigentlichen E-Mail-Kommunikation die Identitätsprüfung von Mailservern und die Feststellung, ob TLS verwendet wird. Durch die Implementierung von DANE ist sichergestellt, dass die Kommunikation verschlüsselt wird. Dabei schützt DANE insbesondere davor, dass durch Manipulation bei der Aushandlung der Kommunikationssicherheit diese auf ein unsicheres Niveau reduziert wird (sog. Downgrade-Attacke).

Bei DANE werden Signaturen (DNS-Fingerprints) zur Verifikation der Zertifikate des Mail-Servers auf DNS-Servern veröffentlicht. Hierfür wird die DNS-Sicherheitserweiterung Domain Name System Security Extensions (DNSSEC) verwendet und bildet daher eine wichtige Voraussetzung für DANE. Nur mit DNSSEC lässt sich gewährleisten, dass die DANE-Angaben im DNS-Record korrekt sind. Für manche EMDA stellt die Implementierung von DNSSEC eine größere Herausforderung dar, da die DNS-Einträge ihrer Domains angepasst werden müssen.

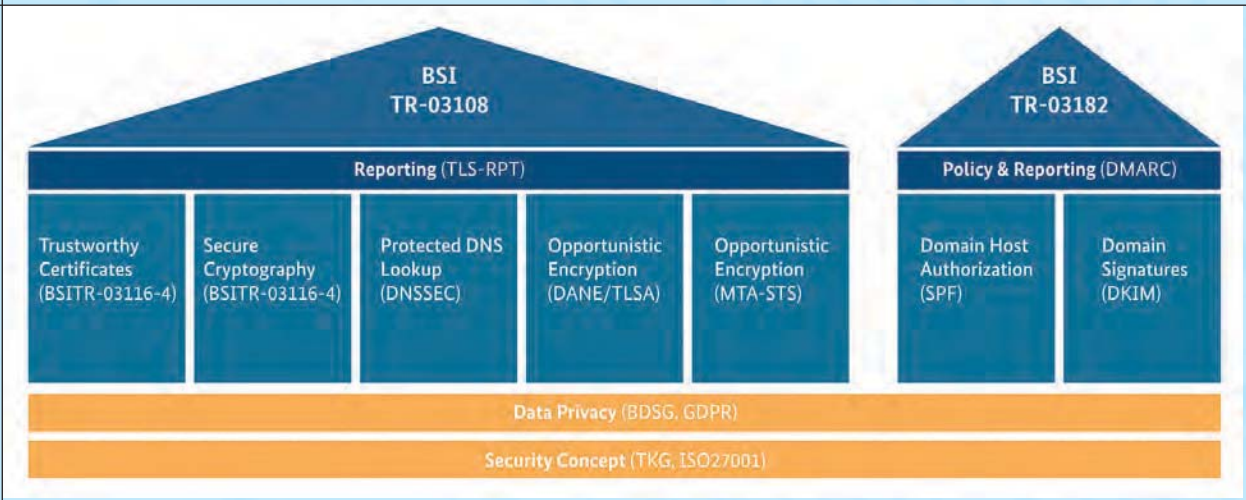
Als Alternative zu DANE mit DNSSEC, wurde deshalb der Standard Mail Transfer Agent-Strict Transport Security (MTA-STS) als zusätzliche Option in die Version 2.0 der TR-03108 aufgenommen. Mittels MTA-STS kann ein EMDA einem anfragenden Mailserver per HTTPS mitteilen, dass eine TLS-gesicherte Verbindung unterstützt wird und sich das verwendete Zertifikat über den MTA-STS-Server verifizieren lässt. MTA-STS ist einfacher implementierbar, bietet aber ein geringeres Schutzniveau als DANE, da dieses abhängig von der Sicherheit des MTA-STS-Servers ist. Aus diesem Grund ist MTA-STS nur als Empfehlung in der TR enthalten.

Anforderungen an authentische E-Mails

In der BSI TR-03182 werden erstmals Anforderungen an authentische E-Mails formuliert. Mit aktuellen Verfahren, wie Domain Keys Identified Mail (DKIM) und Sender Policy Framework (SPF), wird die Identität einer Senderdomain überprüft. Durch diese Maßnahmen sollen SPAM, Spoofing und Phishing erschwert werden. Mit Domain-based Message Authentication, Reporting and Conformance (DMARC) wird auch in dieser TR ein Reporting-Mechanismus als Voraussetzung für die Konformität zur TR eingefordert. DMARC, genau wie auch TLS RPT, ermöglicht es den EMDA, ihre Sicherheitsmaßnahmen kontinuierlich zu optimieren, indem die Kommunikationspartner sich gegenseitig aktiv auf Probleme hinweisen. Die Veröffentlichung der TR-03182 ist bis Ende dieses Jahres geplant.

IT-Sicherheitskennzeichen und Zertifizierung

Auf Basis der TR-03108 (Version 1.0.2) erteilt das BSI das IT-Sicherheitskennzeichen. Durch eine Herstel-



Aufbau der TR-03108 und TR-03182 (Bild: BSI)

lererklärung sichert ein EMDA zu, die verpflichtenden Anforderungen der TR zu erfüllen. Im Rahmen der Antragstellung macht der EDMA insbesondere Angaben zu technischen Eigenschaften des Dienstes und zur angewandten Testmethode. Das BSI führt auf Basis der Angaben eine Plausibilitätsprüfung durch und ermittelt, ob relevante Schwachstellen in diesem Bereich bekannt sind. Nach positiver Prüfung wird das Kennzeichen für die Dauer von zwei Jahren erteilt.

Danach unterliegen alle Geräte mit einem IT-Sicherheitskennzeichen der BSI-Marktaufsicht. Diese kann anlasslos (stichprobenartig) oder anlassbezogen (z. B. bei Bekanntwerden von Schwachstellen) prüfen, ob der EMDA während der Laufzeit die technischen Anforderungen für seinen Dienst erfüllt. Werden durch die Marktaufsicht oder Dritte sicherheitsrelevante Schwachstellen entdeckt, ist der EMDA verpflichtet, diese zu beheben. Über einen QR-Code oder einen Link auf dem jeweiligen Kennzeichen kann eine individuelle Produktinformationsseite auf der Website des BSI aufgerufen werden, die aktuelle Sicherheitsinformationen enthält. Das IT-Sicherheitskennzeichen kann für unterschiedliche Produktkategorien beantragt werden, darunter auch für den großen Bereich der smarten Verbrauchergeräte. In der Kategorie E-Mail-Dienste sind derzeit bereits 18 deutsche E-Mail-Produkte gekennzeichnet.

Zusätzlich zum IT-Sicherheitskennzeichen können EMDA sich die Erfüllung der Anforderungen der TR-03108 (Version 2.0) durch ein Zertifikat von einer unabhängigen Prüfstelle bestätigen lassen. Das BSI hat dafür ein neues Zertifizierungsverfahren aufgesetzt. Ab sofort können beim BSI für die TR-03108 anerkannte Prüfstellen die Diensteanbieter auf Konformität prüfen. Im Erfolgsfall wird die Zertifizierung anschließend durch das BSI vorgenommen. Dieses Verfahren wird zunächst für die TR-03108 (Version 2.0) angeboten.

Mithilfe des IT-Sicherheitskennzeichens und der Zertifizierung erhalten Nutzerinnen und Nutzer eine praktische Orientierungshilfe für die Suche nach einem sicheren E-Mail-Dienst. Gleichzeitig werden den EMDA Anreize geboten, auf dem Markt durch die Verbesserung ihrer Sicherheitsmaßnahmen einen Wettbewerbsvorteil zu erhalten. So können Hersteller und Diensteanbieter das Versprechen in die Sicherheit ihrer Produkte und Dienste sichtbar machen. Verbraucherinnen und Verbraucher können die bereitgestellten Informationen schon vor der Kaufentscheidung berücksichtigen.

Internationale Zusammenarbeit

Da die E-Mail-Kommunikation keine nationalen Grenzen kennt, engagiert sich das BSI auch international und steht mit den europäischen Kolleginnen und Kollegen im regelmäßigen Austausch. Die europäische Arbeitsgruppe „Modern E-Mail Security Standards for EU Governments“ (MESSEU) wurde neben den nationalen Fachverbänden ebenfalls in die Kommentierungsrunden der in englischer Sprache verfassten Richtlinien einbezogen. So wurde sichergestellt, dass die Vorgaben in den Richtlinien praxisnah, zukunftssicher und auch international anwendbar sind.

Fazit

Trotz zunehmender Verbreitung von Messenger-Diensten ist die E-Mail vor allem im geschäftlichen Bereich eines der wichtigsten Kommunikationsmittel. Mit seinen technischen Richtlinien leistet das BSI einen wichtigen Beitrag zur Förderung der sicheren und authentischen E-Mail-Kommunikation für Staat, Wirtschaft und Gesellschaft in Zusammenarbeit mit nationalen und europäischen Partnern. EMDA können die erfolgreiche Umsetzung der Anforderungen durch die vom BSI angebotenen Labelling- und Zertifizierungsverfahren nachweisen und tragen auf diese Weise zu mehr Transparenz ihrer eingesetzten Sicherheitsverfahren gegenüber den Nutzerinnen und Nutzern bei. Ein Verzeichnis der erteilten IT-Sicherheitskennzeichen ist unter www.bsi.bund.de/it-sik/suche einsehbar. Mehr Informationen über eine Anerkennung als TR-Prüfstelle gibt es unter www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Zertifizierung-und-Anerkennung/Anerkennung-von-Stellen-und-Zertifizierung-IT-Sicherheitsdienstleister/TR/tr_node.html.

T-Sicherheitskennzeichen des BSI (Bild: BSI)