Auszug aus <kes> – Die Zeitschrift für Informations-Sicherheit, Ausgabe 2017 #3, www.kes.info

SPF, DKIM, DMARC und DANE:

E-Mail-Sicherheit durch geschützte Zustellung

Die Nutzung von Senderreputationsverfahren zur Absicherung der E-Mail-Kommunikation ist leider noch immer wenig verbreitet – obwohl sich damit ein erheblicher Teil der Spam- und Malware-Attacken abwehren ließe und der Einsatz kostenfrei ist. Dieser Artikel erläutert Nutzen und Funktionsweise der Standards und gibt Tipps zur Umsetzung.

Von Stefan Cink, Paderborn

Das Spam- und Malware-Aufkommen in der E-Mail-Kommunikation ist enorm – prominente Beispiele wie die Ransomware „WannaCry" sind nur die Spitze des Eisbergs. Nach wie vor sind E-Mails generell das wichtigste Einfallstor für Späh- und Schadsoftware (vgl. <kes> 2016#4, S. 53). Vor diesem Hintergrund ist es unverständlich, dass nach wie vor keine flächendeckende oder auch nur überwiegende Nutzung moderner Schutzmechanismen auf Basis von (Ab-/Ver-) Sender- und Empfängerreputation erfolgt.

Namhafte Akteure wie beispielsweise 1&1, Paypal und Microsoft setzen Standards zur Senderidentifikation bereits ein und auch der TeleTrusT – Bundesverband IT-Sicherheit empfiehlt die Nutzung. Die Verfahren sind auf der Basis einheitlicher Standards technisch gut etabliert und seit Jahren bekannt – sie arbeiten automatisiert, bieten mit vergleichsweise geringem Aufwand ein erhebliches Plus an Sicherheit und sind auch ohne teure Werkzeuge umzusetzen.

Standards im Überblick

Die automatische Absenderidentifikation ermöglicht es dem empfangenden Server einer E-Mail, eindeutig festzustellen, ob eine Nachricht tatsächlich von dem Absender stammt, von dem sie zu sein vorgibt. Darüber hinaus kann er feststellen, ob der einliefernde Server autorisiert ist, im Namen der absendenden Domain E-Mails zuzustellen. Möglich wird dies durch die Verwendung spezieller Methoden zur Absenderidentifikation, die aufeinander aufbauen:

- SPF: Sender-Policy-Framework (RFC 7208, [1])
- DKIM: Domain-Keys-Identified-Mail (RFC 6376, [2])
- DMARC: Domain-based Message-Authentication, Reporting and Conformance (RFC 7489, [3])

Mit der „DNS-based Authentication of Named Entities" (DANE, RFC 6698, [4]) kommt ein Verfahren zur Validierung des Empfängers ergänzend hinzu.

Damit diese Methoden ihre volle Wirkung entfalten können, müssen allerdings zwei Dinge zusammenkommen: Zum einen müssen Domainverwalter die entsprechenden SPF-, DKIM-, DMARC- und DANE-Informationen für die eigenen Domains veröffentlichen und damit externen Kommunikationspartnern bekannt machen. Zum anderen sollten alle empfangenden Unternehmen E-Mail-Security-Lösungen einsetzen, welche die genannten Informationen auch konsequent nutzen. Dann können die empfangenden Kommunikationspartner zweifelsfrei feststellen, dass eine E-Mail tatsächlich unverändert ist und vom korrekten Absender kommt.

Außerdem profitiert der Versender vom zusätzlichen Nutzen eines deutlich reduzierten Risikos von Reputationsverlusten für die eigenen Domains und sollte diese Methoden daher schon aus diesem Grund einsetzen.

Wirksam im Quartett

Erst die Kombination aller vier Elemente bietet jedoch einen wirksamen Schutz der E-Mail-Kommunikation: So ist die alleinige Nutzung von SPF-Records bei der Prüfung eingehender E-Mails nur bedingt hilfreich. Denn das Abweisen einer E-Mail lediglich aufgrund einer fehlgeschlagenen SPF-Prüfung würde unter Umständen auch valide E-Mails verwerfen, die weitergeleitet oder über eine Mailingliste verschickt wurden. Beide Szenarien führen zu Fehlern bei der SPF-Prüfung, weil der weiterleitende Server in der Regel nicht im SPF-Record der ursprünglichen Absender-Domain gelistet ist.

Dieses Problem wird beispielsweise durch den Einsatz von DKIM entschärft: Beim ursprünglichen Versand einer E-Mail wird diese um eine DKIM-Signatur

© DATAKONTEXT GmbH · 50226 Frechen · <kes> 2017#3

angereichert, die im Header der E-Mail verankert wird – wird sie von den im weiteren Verlauf beteiligten Relay-Servern nicht entfernt, kann der Zielserver sie erfolgreich überprüfen. Im Szenario „Weiterleitung einer E-Mail“ würde der empfangende Server somit feststellen, dass die SPF-Prüfung zwar fehlschlägt, die E-Mail aber über eine gültige DKIM-Signatur verfügt, also unverfälscht übermittelt wurde.

Die Ergebnisse der SPF- und DKIM-Prüfung lassen aber noch immer offen, welche Behandlung einer „durchgefallenen“ E-Mail der Absender empfiehlt. Diese Lücke schließt die Auswertung der DMARC-Richtlinie der Absender-Domain: Diese erklärt zweifelsfrei, mit welchen Verfahren ausgehende E-Mails wie geschützt sein müssen und wie im Fehlerfall mit ihnen umzugehen ist. Des Weiteren kann der sendende Domain-Inhaber über die Ergebnisse der Prüfung informiert werden.

Liegen auch DANE-Information vor, lässt sich überdies sicherstellen, dass kein Angreifer zwischen Sender und Empfänger als Man-in-the-Middle agieren kann, indem eine vertrauenswürdige, TLS-verschlüsselte Verbindung aufgebaut wird.

Angriffsvektoren ausgehebelt

Eine vollständige Nutzung der Möglichkeiten der Senderreputation liefert – kombiniert mit DANE zum Zwang zur verschlüsselten Übertragung – einen verlässlichen Schutz gegen weitverbreitete Angriffsmuster, die oft von gängigen Schutzmechanismen nur unzulänglich unterbunden werden.

Bei der Chef-Betrugsmasche (CEO-Fraud) ergibt sich dann beispielsweise, dass die bewusste E-Mail nicht – wie vorgegaukelt – vom eigenen Chef kommen kann: Sie fällt bei der Absenderprüfung durch, da sie ja nur vorgeblich der eigenen Domäne entstammt und damit nicht die richtigen Merkmale bei SPF, DKIM und DMARC erfüllen kann.

Auch gegen viele Phishing-Angriffe zum Abgreifen von Zugangsdaten oder Malware-Attacken mit Downloadlinks wirkt die Auswertung der Absenderreputation: Egal wie gut eine Betrugsmail optisch und inhaltlich gemacht ist, fällt sie doch bei der Prüfung der Absendermerkmale durch, wenn Sender und Empfänger sie konsequent nutzen.

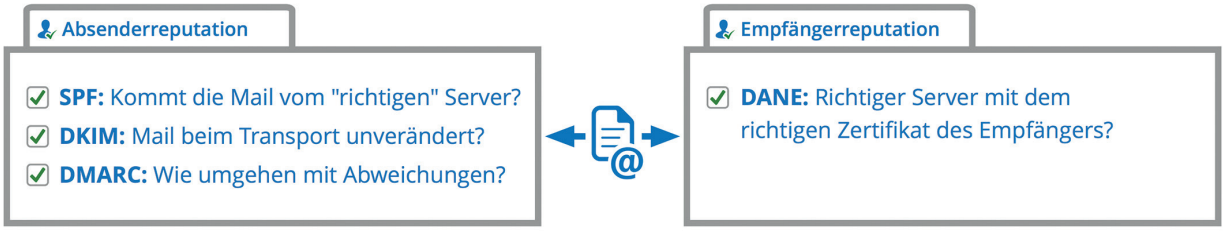
Ein gutes Beispiel sind Betrugsversuche im Zusammenhang mit PayPal: Zwar zeigen die teilweise perfekt gefälschten Mails für den Nutzer – basierend auf der Information im „Body-From“-Header der E-Mail – PayPal als Absender an. Im „Envelope-Sender“ steht jedoch die wirklich versendende Domain. Da PayPal seine Domains mit einem DMARC-Record schützt, kann ein empfangendes E-Mail-Gateway diesen Betrugsversuch sicher erkennen – sofern es denn diese wertvollen Informationen auswertet.

Gerade das Beispiel PayPal zeigt eindrucksvoll, wie wichtig die Prüfung der Absender-Domain im Rahmen einer intelligenten E-Mail-Security geworden ist. Anders als die oft verwendeten pattern- oder sandboxbasierten Verfahren, unterliegen die Absenderreputationsverfahren nicht dem vielzitierten „Hase-und-Igel-Spiel“ zwischen Angreifern und Sicherheitssoftware. Die Prüfung erfolgt zudem in Echtzeit und ermöglicht so eine zeitnahe Zustellung der E-Mail.

Tipps zur Einführung

Jede Einführung neuer Verfahren birgt naturgemäß gewisse Risiken. Wird bei der Einrichtung und Pflege von SPF, DKIM, DMARC und DANE nicht sorgfältig gearbeitet, können im schlimmsten Fall Unterbrechungen des E-Mail-Verkehrs auftreten. Hier bieten sich zwei Hilfestellungen an: Einerseits unterstützen gute Secure-E-Mail-Gateways ihren Administrator bei der Einrichtung und Pflege von DMARC & Co. – doch auch ohne teure Tools kann jeder qualifizierte Mail-Admin diese Einstellungen selbst vornehmen. Und beispielsweise bietet Net at Work auf ihrer Website auch einen kostenlosen Praxisleitfaden an, der die Einrichtung Schritt für Schritt erklärt [5]. Im Internet stehen überdies einige freie Tools zur Verfügung, um entsprechende DNS-Records einzurichten oder zu prüfen (u. a. [6,7,8,9,10]).

Die Überwachung der SPF- und DKIM-Records erfolgt sinnvollerweise mithilfe der DMARC-Reports, die automatisch zugeschickt werden. Zur Auswertung des zuweilen umfangreichen Reports empfehlen sich gegebe-



Spezielle Methoden zur Absender- und Empfängeridentifikation bieten wertvolle Hilfe im Kampf gegen Spam und Malware.

nenfalls kommerzielle Tools wie DMARCIAN, Agari oder ReturnPath – so kann der Verwalter einer Domain schnell erkennen, welche Server E-Mails von der eigenen Domain abgelehnt haben und aus welchem Grund. Mögliche Lücken im SPF-Record können so schnell gestopft werden. Zudem erkennt der Verwalter einer Domain, wie häufig Betrugsversuche unter Vorgaukeln der eigenen Domain im Netz auftreten und kann entsprechende Kommunikationsmaßnahmen an die Kunden auslösen – auch das schützt die eigene Reputation.

Standards für vertrauenswürdige E-Mails

Für das Verständnis der nachfolgenden Konzepte ist es wichtig, den Unterschied zwischen dem so genannten Envelope-Sender und dem Body-From-Absender einer E-Mail zu kennen:

Als Envelope-Sender wird die E-Mail-Adresse bezeichnet, die während eines SMTP-Handshakes übergeben wird. Die Bezeichnung Envelope ist in Anlehnung an den Briefumschlag gewählt: Wie bei der Briefpost ist nur das, was auf dem Umschlag steht, für den Transport ausschlaggebend. Wie bei der Briefpost wird der Absender auf dem Umschlag (Envelope-Sender) darüber informiert, wenn seine Nachricht nicht zustellbar war – unabhängig davon, welcher Absender in der Nachricht selbst genannt wird.

Die Absenderinformation in Form des Body-From ist zum einen im Body, genauer gesagt im Header der E-Mail, enthalten und umfasst neben der eigentlichen E-Mail-Adresse in der Regel noch weitere Informationen zum Absender wie Vor- und Nachname oder den Namen des Postfachs. E-Mail-Programme (Mail-User-Agents, MUAs) zeigen häufig nur den Body-From an. E-Mails aus dem Postfach des Autors werden im Posteingang des Empfängers beispielsweise als gesendet von „Max Muster“ und nicht von „max.muster@example.com“ angezeigt.

Sender-Policy-Framework (SPF)

Im Sender-Policy-Framework (SPF, RFC 7208, [1]) gibt der Inhaber einer Domain im Domain-Name-System (DNS) an, welche Server autorisiert sind, E-Mails im Namen der eigenen Domain zu versenden. Dazu erstellt er in der entsprechenden DNS-Zone einen so genannten SPF-Record – technisch gesehen ein TXT-Record, dessen Syntax in RFC 7208 spezifiziert ist.

Bei der Zustellung einer E-Mail entnimmt der empfangende Server die Absender-Domain aus dem Envelope-Sender einer E-Mail. Anschließend wird im Rahmen einer DNS-Abfrage ermittelt, ob für die Domain ein SPF-Record existiert. Diese Prüfung wird optional zusätzlich für den Host-Eintrag des Absenders (EHLO-Client-ID) durchgeführt. Taucht die IP-Adresse oder FQDN des einliefernden Servers nicht im SPF-Record auf, ist er für den Versand von E-Mails im Namen dieser Domain nicht autorisiert.

Domain-Keys-Identified-Mail (DKIM)

Bei Domain-Keys-Identified-Mail (DKIM, RFC 6376, [2]) wird ebenfalls ein TXT-Record mit RFC-normierter Syntax in der DNS-Zone der zu schützenden Domain erstellt. Zusätzlich kommt hierbei per Signatur mit einem Public-Key-Verfahren eine kryptografische Komponente zum Tragen. Anders als bei SPF wird bei DKIM die Absender-Domain aus dem Body-From einer E-Mail untersucht.

Vor der Erstellung des DKIM-Records wird ein Schlüsselpaar erstellt – der öffentliche Schlüssel wird in Kombination mit anderen Informationen als DKIM-Record in der DNS-Zone hinterlegt. Der geheime Schlüssel verbleibt ausschließlich auf dem Server, der für den Versand autorisiert werden soll. Mit diesem Schlüssel erzeugt der absendende Server für jede ausgehende E-Mail eine kryptografische Signatur, die sowohl Teile des Headers als auch den Inhalt der E-Mail erfasst. Idealerweise verfügt der Server über jeweils einen anderen Schlüssel für jede Domain, für die er E-Mails versenden soll. Die erzeugte DKIM-Signatur wird als X-Header-Wert in die jeweilige E-Mail geschrieben.

Der empfangende Server ermittelt zunächst die Absender-Domain der Nachricht, gefolgt vom so genannten Selektor: Der Selektor ist fester Bestandteil einer DKIM-Signatur und gibt an, unter welchem Namen der passende öffentliche Schlüssel in der DNS-Zone der Absender-Domain zu finden ist. Nach dem Download des passenden öffentlichen Schlüssels wird die Signatur geprüft: Schlägt diese Prüfung fehl, liegt entweder der falsche öffentliche Schlüssel vor oder die E-Mail wurde unterwegs verändert.

Eine erfoglreiche DKIM-Signatur-Prüfung stellt somit zwei Dinge sicher: Zum einen weiß der empfangende Server, dass die E-Mail samt Inhalt auf dem Transportweg nicht verändert wurde. Zum anderen weiß er, dass der Inhaber der im Header (Body-From) angegebenen Absender-Domain den Server zum Versand autorisiert hat.

Anders als bei kryptografischen Signaturen mittels S/MIME oder PGP sieht der Empfänger einer E-Mail die DKIM-Signatur jedoch normalerweise nicht – es handelt sich um ein rein serverbasiertes Verfahren. Nur wenn

© DATAKONTEXT GmbH · 50226 Frechen · <kes> 2017#3

Zögerliche Unterstützung

Vor Kurzem hat die TeleTrusT European Bridge CA (EBCA – ein PKI-Verbund gleichberechtigter Public-Key-Infrastrukturen) DANE als wichtige Ergänzung für die Transportverschlüsselung mit TLS-Verbindungen empfohlen. Auch auf dem gerade zu Ende gegangenen 15. Deutschen IT Sicherheitskongress des BSI in Bonn (vgl. S. 27) wurden Sender- und Empfängerreputation thematisiert. Ein Blick auf den Security-Markt zeigt aber, dass

man sich den Header einer E-Mail anzeigen lässt, wird die DKIM-Signatur sichtbar.

Domain-based Message-Authentication, Reporting and Conformance (DMARC)

Weder SPF noch DKIM geben dem empfangenden Server einer E-Mail klare Anweisungen, was mit E-Mails passieren soll, bei denen die SPF- und/oder DKIM-Prüfung nicht erfolgreich verläuft – diese Lücke schließt DMARC (RFC 7489, [3]).

DMARC ergänzt die SPF- und DKIM-Prüfungen um das so genannte Alignment: Es stellt sicher, dass die Envelope-Sender-Adresse mit der Body-From-Adresse übereinstimmt. Diese Prüfung ist wichtig, weil die gängigsten E-Mail-Programme lediglich die Body-From-Informationen einer E-Mail anzeigen und der Empfänger somit leicht getäuscht werden kann.

Eine weitere Besonderheit von DMARC ist die Berichtsfunktion: Sie sorgt dafür, dass der Inhaber einer Domain regelmäßig darüber informiert wird, welche Server in seinem Namen E-Mails versendet haben und ob die Prüfung beim Empfänger erfolgreich war oder nicht. So bekommt er nicht nur einen guten Überblick über „seine" E-Mails im Internet, sondern auch wertvolle Informationen darüber, ob seine SPF- und DKIM-Einträge vollständig und syntaktisch korrekt sind.

Um DMARC zu aktivieren, hinterlegt der Inhaber einer Domain eine DMARC-Richtlinie in seiner DNS-Zone. Wie bei SPF und DKIM auch, wird die DMARC-Richtlinie in einem RFC-normierten TXT-Record gespeichert. Sie enthält Angaben dazu, welche Prüfungen ein Empfänger durchführen soll (SPF und/oder DKIM) – und wie sich der Empfänger verhalten soll, wenn die Prüfungen fehlschlagen: Annehmen, in Quarantäne stecken oder Abweisen sind die möglichen Aktionen.

Des Weiteren werden in der DMARC-Richtlinie E-Mail-Adressen hinterlegt, an die Berichte geschickt werden sollen. Diese werden von allen Servern im Internet erstellt, die DMARC beim E-Mail-Empfang unterstützen und auch E-Mails von der jeweiligen Domain erhalten haben. Diese Berichterstattung erfolgt täglich. Um das Berichtsaufkommen begrenzen zu können, lässt sich in einer DMARC-Richtlinie auch angeben, dass zum Beispiel nur für jede zehnte E-Mail ein Bericht generiert werden soll – dies ist jedoch nur bei sehr hohem Mail-Volumen zu empfehlen.

DNS-based Authentication of Named Entities (DANE)

Wie alle vorangegangenen Technologien arbeitet auch der DANE-Standard (RFC 6698, [4]) DNS-basiert, stellt aber umfangreichere Anforderungen an die DNS-Umgebung. In einem Satz zusammengefasst, ermöglicht DANE die kryptografische Verknüpfung von Zertifikaten mit DNS-Namen. Der Einsatz von TLS zur Verschlüsselung von Verbindungen zu einem Server ermöglicht lediglich den Schutz vor ungebetenen Mithörern – DANE erweitert diesen Grundschutz um eine sichere Identifizierungs- und Austausch-Funktion.

Ein prominenter Anwendungsfall ist die DANE-Absicherung im Rahmen der TLS-Verschlüsselung zwischen zwei E-Mail-Servern: So soll verhindert werden, dass eine Nachricht durch eine Man-in-the-middle-Attacke zunächst über den E-Mail-Server eines Angreifers laufen kann. Der Inhaber einer Domain legt dazu in der entsprechenden DNS-Zone fest, welches Zertifikat ein Server erwarten muss, wenn dieser sich mit dem E-Mail-Dienst auf dem E-Mail-Server verbindet. Sowohl der gewünschte Name als auch der richtige Port des E-Mail-Servers können mit DANE zweifelsfrei festgelegt werden. Somit weiß der absendende Server nicht nur, dass er mit dem richtigen Ziel-Server eine Verbindung eingeht, sondern darüber hinaus auch, dass ihm das richtige Zertifikat für die Verbindungsverschlüsselung angeboten wird.

DANE wird zwar auch über einen Eintrag in der DNS-Zone abgebildet, nutzt aber keinen TXT-, sondern einen TLSA-Record. Dieser ist seit Oktober 2015 in RFC 7671 spezifiziert. Des Weiteren muss die DNS-Zone zwingend DNSSEC-geschützt sein, was sicherstellt, dass ein Angreifer die DNS-Antworten nicht zu seinen Gunsten manipulieren kann.

Neben der Absicherung von TLS-Verbindungen zwischen E-Mail-Servern kann DANE prinzipiell auch HTTPS-Verbindungen zu Webservern schützen – ein weiteres Einsatzgebiet ist die Veröffentlichung von E-Mail-Verschlüsselungs-Zertifikaten über DNS. Dieser Artikel fokussiert sich jedoch auf das Einsatzszenario im Bereich der E-Mail-Zustellung.

selbst namhafte Anbieter von E-Mail-Security-Lösungen die umfangreichen Möglichkeiten der Absender- und Empfängervalidierung nicht nutzen.

Dabei lassen sich mit der gezielten Analyse der entsprechenden Informationen deutliche Verbesserungen in Sicherheit und Genauigkeit erreichen. Secure-Mail-Gateways sollten daher die SPF-, DKIM- und DMARC-Einträge des Absenders konsequent auswerten und das Ergebnis mit dem Resultat weiterer Techniken zur Spam- und Malware-Erkennung kombinieren. Für eine noch zuverlässigere Feststellung der Vertrauenswürdigkeit können Gateways auch abgehende E-Mails analysieren und dann beispielsweise erkennen, dass eine eingehende E-Mail von einem Absender stammt, mit dem bereits aktiv und valide kommuniziert wurde.

Die Ergebnisse der Prüfungen können anschließend beispielsweise auch für ein intelligentes Anhangsmanagement herangezogen werden: Denkbar sind hier unterschiedliche Richtlinien für vertrauenswürdige und nicht-vertrauenswürdige Absender. Eine ZIP-Datei von einem zweifelsfrei identifizierten Absender könnte etwa vorbehaltlich einer erfolgreichen Virenprüfung ohne Weiteres zugestellt werden, während sie von einem nicht-identifizierten Absender entweder komplett abgelehnt oder aber zunächst in Quarantäne gestellt werden sollte.

Fazit

Alle Organisationen und Nutzer leiden unter Spam und Malware. Wirksam reduzieren kann man dieses Übel nur, wenn Versender und Empfänger von E-Mails gemeinsam alle Möglichkeiten ausnutzen. Die Nutzung von DMARC & Co. kann ein Meilenstein für Sicherheit und Effizienz in der E-Mail-Kommunikation sein. Die Bewertung der Reputation des Absenders ist ein sehr verlässliches Instrument im Kampf gegen stetig steigende Mengen an Spam und immer perfider werdende Angriffsszenarien mit Malware.

Die Einrichtung der vorgestellten Standards bedarf keiner teuren Tools oder horrenden Aufwands – vor allem braucht es guten Willen und etwas Know-how. So bleibt es zu hoffen, dass schnell wesentlich mehr Organisationen und E-Mail-Administratoren diesen Ball aufgreifen und gemeinschaftlich ein wirksames Mittel gegen Spam- und Malware-Unwesen einsetzen. ■

Stefan Cink ist E-Mail-Security-Spezialist bei der Net at Work GmbH.

Literatur

[1] S. Kitterman, Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1, IETF RFC 7208, April 2014, https://tools.ietf.org/html/rfc7208 – s. a. https://datatracker.ietf.org/doc/search/?name=Sender+Policy&activedrafts=on&rfcs=on

[2] D. Crocker, T. Hansen und M. Kucherawy (Hrsg.), DomainKeys Identified Mail (DKIM) Signatures, IETF RFC 6376, September 2011, https://tools.ietf.org/html/rfc6376 – s. a. https://datatracker.ietf.org/wg/dkim/documents/

[3] M. Kucherawy und E. Zwicky (Hrsg.), Domain-based Message Authentication, Reporting, and Conformance (DMARC), IETF RFC 7489, März 2015, https://tools.ietf.org/html/rfc7489 – s. a. https://datatracker.ietf.org/wg/dmarc/documents/

[4] P. Hoffman, J. Schlyter, The DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA, IETF RFC 6698, https://tools.ietf.org/html/rfc6698 – s. a. https://datatracker.ietf.org/wg/dane/documents/

[5] Net at Work, Praxisleitfaden zur sicheren Prüfung von Senderidentifikationen mit DKIM, SPF, DMARC und DANE, Whitepaper, www.nospamproxy.de/de/ratgeber-dmarc-dkim-spf-dane (Registrierung erforderlich)

[6] Kitterman Technical Services, SPF Record Testing Tools, www.kitterman.com/spf/validate.html

[7] Kitterman Technical Services, DMARC Record Assistant, http://kitterman.com/dmarc/assistant.html

[8] Digineo, SSL-Tools – TLSA Eintrag generieren, https://de.ssl-tools.net/tlsa-generator

[9] sys4, DANE SMTP Validator, https://dane.sys4.de

[10] MxToolbox, Network Tools (incl. SPF, DMARC, DKIM, MX,...), https://mxtoolbox.com/NetworkTools.aspx

[11] Roundsphere, DKIM, SPF, SpamAssassin Email Validator, http://dkimvalidator.com

[12] Patrick Koetter, Johannes Endres, E-Mails signieren mit DKIM, Kryptographie gegen Phishing und Spam, heise Netze, Oktober 2008, http://heise.de/-221505

© DATAKONTEXT GmbH · 50226 Frechen · <kes> 2017#3

Informations-Sicherheit im Abonnement

<kes> liefert alle relevanten Informationen zum Thema IT-Sicherheit – sorgfältig recherchiert von Fachredakteuren und Autoren aus der Praxis.

<kes>

— strategisches Know-how

— Trends und Neuentwicklungen

— Hilfen zum Risikomanagement

— einschlägige Gesetze im Umfeld der IT und TK

— wichtige Messen und Kongresse

— Anwenderberichte

— BSI-Forum

— IT-Grundschutz

Fax-Rückantwort an +49 89 2183-7620

Ich/Wir abonniere(n) die Zeitschrift <kes> ab Ausgabe _____

Das Abonnement umfasst das Recht zur Nutzung des Abo-Bereichs auf www.kes.info mit allen aktuellen Beiträgen und dem **<kes>-Archiv** sowie den Bezug des <kes>/SecuPedia-Newsletters**.**

Jahresbezugspreis (sechs Ausgaben) € 135,00 inkl. MwSt. und Versandkosten (Ausland € 159,30).
Der Bezugszeitraum beträgt ein Jahr. Sie können das Abonnement jederzeit, spätestens jedoch acht Wochen vor Ende des Bezugsjahres kündigen. Sonst verlängert sich das Abo automatisch um ein weiteres Jahr.

Datenschutzhinweis: Ihre persönlichen Angaben werden von der DATAKONTEXT GmbH ausschließlich zur Vertragserfüllung einschließlich Zusendung des Newsletters, evtl. unter Einbeziehung von Dienstleistern, verwendet. Darüber hinaus erfolgt die Weitergabe an Dritte nur zur Vertragserfüllung oder wenn wir gesetzlich dazu verpflichtet sind. Falls Sie keine weiteren Informationen von DATAKONTEXT mehr erhalten wollen, können Sie uns dies jederzeit mit Wirkung in die Zukunft an die DATAKONTEXT GmbH, Augustinusstr. 9d, 50226 Frechen, per Fax an +49 2234 98949-44 oder per E-Mail an werbewiderspruch@datakontext.com mitteilen.

* erforderlich zur Zusendung des Secupedia-Newsletters – zusätzlich erhalten Sie Informationen zu eigenen ähnlichen Produkten per E-Mail. Sie können dieser Ansprache jederzeit widersprechen, ohne dass hierfür andere als die Übermittlungskosten nach den Basistarifen entstehen.

Online-Bestellung über http://abo.kes.info

QR-Code für Bestellung per E-Mail

Firma _____ Abteilung _____

Name/Vorname _____

E-Mail* _____

Telefon (Geschäftl.) _____ Fax (freiwillige Angabe) _____

Straße/Nr. _____

PLZ/Ort _____

Datum/Unterschrift _____