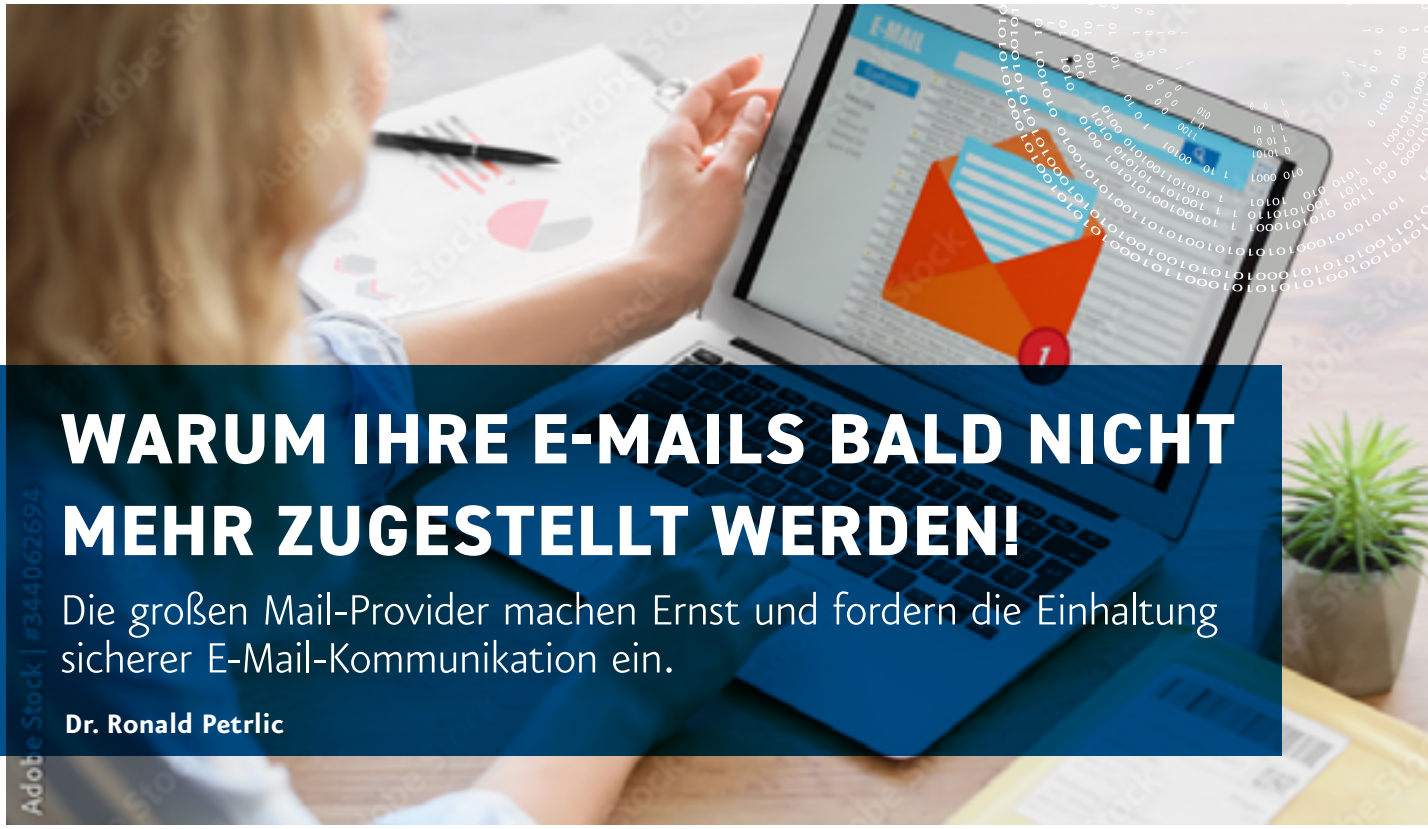

WARUM IHRE E-MAILS BALD NICHT MEHR ZUGESTELLT WERDEN!

Die großen Mail-Provider machen Ernst und fordern die Einhaltung sicherer E-Mail-Kommunikation ein.

Dr. Ronald Petrlic

Spam / Phishing / Ransomware

Die E-Mail ist seit Jahren Einfallstor Nummer 1 für Angriffe. Aus früheren Jahren sind noch die E-Mails bekannt, die in schlechtem Deutsch die Nutzer dazu aufforderten, dubiose Webseiten zu besuchen, personenbezogene Daten preis zu geben, bei Gewinnspielen teilzunehmen und in Fake-Shops einzukaufen. Auf diese Spam-E-Mails fällt heute kaum noch jemand herein.

In den vergangenen Jahren wurden diese E-Mails jedoch immer ausgereifter. Das Ziel der Angreifer ist häufig Phishing. Die Empfänger werden mit echt aussehenden E-Mails dazu gebracht, auf die in den E-Mails enthaltenen Links zu klicken und auf der ebenfalls echt aussehenden Website ihre Zugangsdaten einzugeben. Viele Angriffe richten sich an Unternehmen, wobei der E-Mail-Account dr Mitarbeitenen Ziel des Angriffs ist. Fällt ein Mitarbeiter darauf rein und gibt auf der gefakten Exchange-Online-Seite seine Zugangsdaten ein, ist dies der Jackpot für den Angreifer. Er hat damit Zugriff auf sämtliche E-Mail-Kommunikation des Mitarbeiters sowie Zugang zu den Kontakten und Terminen des Opfers. Dies ist häufig der erste Schritt für weitergehende Angriffe auf das Unternehmen. Bekannt sind derartige Angriffe auch – und vor allem - aus dem Umfeld des Online-Bankings, bei dem vermeintlich die Bank die Kunden per E-Mail dazu auffordert, sich online anzumelden.

Daneben werden Unternehmen von einer weiteren Art von Angriffen geplagt: Ransomware. Auch hier ist das typische Einfallstor die E-Mail. Kampagnen mit Angreifern wie Emotet haben in den zurückliegenden Jahren zahlreiche Unternehmen, Arztpraxen, Behörden und Krankenhäuser lahmgelegt. Eine Unachtsamkeit eines Mitarbeiters reicht dabei. Durch das Ausführen einer an die E-Mail angehängten Datei verbreitet sich die Schadsoftware im gesamten Netzwerk der Organisation und verschlüsselt sämtliche Dateien, Backup inklusive. Die Auswirkungen dieser Angriffe ließen sich zwar vermeiden, doch viele Organisationen haben keine ausreichenden Sicherheitsmaßnahmen etabliert.

Wo liegt das Problem?

Das Problem liegt darin, wie die E-Mail-Kommunikation funktioniert. Das zugrundeliegende SMTP-Protokoll bietet keinerlei Schutzmechanismen. Weder wird die Vertraulichkeit gewahrt noch die Integrität und Authentizität. Über das Thema Vertraulichkeit haben wir in der BvD News 3/22 bereits berichtet.

In diesem Beitrag geht es nicht um Vertraulichkeit, sondern um Authentizität! Der Sender einer E-Mail kann den Absender beliebig fälschen. Dies geht sogar so weit, dass der Sender nicht nur den in der E-Mail angezeigten Absender-Namen fälschen kann, sondern sogar im Namen einer anderen Organisation E-Mails versenden kann. Und gerade das macht es für die Empfänger so schwer, die Legitimität einer empfangenen E-Mail zu prüfen. Wenn eine empfangene E-Mail die En-

dung „@bvdnet.de“ hat, dann kommt diese E-Mail aus Sicht vieler Nutzer auch vom BvD. In Wirklichkeit stammt sie jedoch vom Angreifer.

Gibt es keinen Schutz vor solchen Angriffen?

Doch, den gibt es! Es gibt drei Verfahren, die seit Jahren etabliert sind (die entsprechenden „Standardisierung“-RFCs sind älter als 10 Jahre!) und die heute von allen E-Mail-Servern in der Praxis unterstützt werden: SPF, DKIM und DMARC.

SPF: Das Sender Policy Framework erlaubt es dem Inhaber einer Domain (beispielsweise „bvdnet.de“), im Domain Name System (DNS) einen Eintrag zu hinterlegen, in dem festgehalten wird, von welchem E-Mail-Server aus E-Mails „im Namen des BvD“ (also mit der Endung @bvdnet.de) versendet werden dürfen. Diese Festlegung basiert auf IP-Adressen. Geprüft wird dabei beim Empfang einer E-Mail: Der empfangende E-Mail-Server sieht, dass eine E-Mail vermeintlich von bvdnet.de eingeht. Der Server prüft, ob bvdnet.de einen SPF-Eintrag im DNS hinterlegt hat. Ist dies der Fall, prüft der Mail-Server, ob die IP-Adresse aus dem Eintrag mit jener des E-Mail-Servers übereinstimmt, der die E-Mail gerade einliefert. Stimmen die IP-Adressen nicht überein, handelt es sich bei der E-Mail um eine E-Mail mit gefälschtem Absender und der E-Mail-Server kann die E-Mail direkt verwerfen, ohne sie dem Empfänger zuzustellen.

DKIM: Das Domain Keys Identified Mail-Protokoll stellt einen weiteren Baustein zur Sicherstellung der Authentizität in der E-Mail-Kommunikation dar. Der sendende E-Mail-Server signiert dabei ausgehende E-Mails mit seinem privaten Schlüssel. Der zugehörige öffentliche Schlüssel wird wiederum im DNS abgelegt. Geprüft wird auch bei DKIM wieder beim empfangenden E-Mail-Server. Dieser prüft, ob die Signatur der eingehenden E-Mail gültig ist, also ob sie tatsächlich vom behaupteten E-Mail-Server stammt und ob sie auf dem Transportweg nicht manipuliert wurde. Den zur Prüfung nötigen öffentlichen Schlüssel besorgt sich der empfangende E-Mail-Server aus dem DNS. Stimmt die Signatur nicht, kann die E-Mail direkt verworfen werden.

DMARC: Die Domain-based Message Authentication, Reporting and Conformance-Spezifikation baut auf SPF und DKIM auf. Es erlaubt dem Inhaber einer Domain, im DNS einen Eintrag zu hinterlegen, der spezifiziert, wie ein empfangener E-Mail-Server reagieren soll, wenn die SPF- und/oder DKIM-Prüfung bei einer eingehenden E-Mail fehlschlägt. Erhält der eingehende E-Mail-Server also beispielsweise eine E-Mail, die vermeintlich von bvdnet.de stammt, wobei eine oder beide Prüfungen (SPF/DKIM) fehlschlagen, erkennt der E-Mail-Server am Eintrag aus dem DNS von bvdnet.de, wie er die E-Mail behandeln soll. Hat der BvD korrekterweise einen „reject“-Eintrag im DNS hinterlegt, wird der empfangende E-Mail-Server die gefälschte E-Mail korrekterweise verwerfen. Außerdem versendet der empfangende E-Mail-Server an alle sendenden E-Mail-Server täglich einen aggregierten Bericht darüber, wie viele E-Mails von dieser Domain akzeptiert wurden und wie viele E-Mails die SPF/DKIM-Prüfung nicht bestanden haben und somit aussortiert wurden.

An dieser Stelle sei noch einmal explizit darauf hingewiesen, dass die drei Verfahren ausschließlich in der E-Mail-Infrastruktur umgesetzt werden, also auf den in der Kommunikation beteiligten E-Mail-Servern sowie auf den DNS-Servern. Im Gegensatz zu Verfahren wie PGP oder S/MIME, bei denen die Nutzer aktiv werden müssen, ist dies bei SPF, DKIM und DMARC nicht der Fall! Die drei Verfahren haben wie dargelegt die Authentizität zum Ziel und nicht die Vertraulichkeit.

Wie steht es um die Umsetzung in der Praxis?

Die in der Praxis genutzten E-Mail-Server unterstützen alle drei Verfahren. Die großen Mail-Provider sowie die meisten E-Mail-Server von Unternehmen nutzen zu-

mindest SPF und DKIM. Wobei die konkreten Einstellungen in vielen Fällen nicht optimal sind und die Verfahren damit nicht den gewünschten Nutzen bringen. In einer Studie wurde 2021 festgestellt, dass nur 16 von 37 deutschen Webhosting-Anbietern DKIM umsetzen und nur 6 fehlerfrei konfiguriert waren (Quelle: Leo Dessani, Jan Mahn: DKIM-Fail. Fehler bei Hostern gefährden die Sicherheit von DKIM. In: c't. Nr. 1, 2021, S. 126-129). Bei DMARC gibt es noch mehr Handlungsbedarf: In unserer Untersuchung von rund 60.000 E-Mail-Servern von Unternehmen haben wir festgestellt, dass 67 Prozent überhaupt kein DMARC unterstützen und nur 2 Prozent mit „reject" die richtige Policy haben. Mehr Details zu unserer Auswertung werden wir unter www.mail-sicherheit.jetzt publizieren.

Was fordern die Aufsichtsbehörden?

Die Datenschutz-Aufsichtsbehörden haben im Jahr 2020 eine Orientierungshilfe zur E-Mail-Sicherheit veröffentlicht, die 2021 aktualisiert wurde (Quelle: DSK: Orientierungshilfe der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 27. Mai 2021. „Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail").

In Bezug auf die Authentizität in der E-Mail-Kommunikation fordern die Behörden: „…sollten Verantwortliche DKIM-Signaturen prüfen und signierte Nachrichten, bei denen die Prüfung fehlschlägt, markieren oder, bei entsprechender Festlegung des Absenders über einen DMARC-Eintrag im DNS, zurückweisen."

Bislang ist nicht bekannt, dass die Datenschutz-Aufsichtsbehörden verantwortliche Stellen dazu aufgefordert hätten, SPF/DKIM und DMARC richtig umzusetzen. Die Behörden beschäftigen sich bei der E-Mail-Kommunikation fast ausschließlich mit Fragestellungen zur Vertraulichkeit (insbesondere der Ende-zu-Ende-Verschlüsselung). Die Frage der Authentizität wird leider außer Acht gelassen. Dies hat zur Folge, dass verantwortliche Stellen in diesem Bereich nicht aktiv werden – obwohl eine Umsetzung der beschriebenen Verfahren einen wichtigen Baustein für die Sicherheit der Organisationen darstellen würde, da damit gefälschte E-Mails automatisch aussortiert werden könnten.

Warum sollen E-Mails plötzlich nicht mehr zugestellt werden?

Die großen E-Mail-Provider werden aktiv und fordern von E-Mail-Server-Betreibern die Umsetzung von SPF/DKIM und DMARC. Gmail und Yahoo als weltweit führende Mail-Provider haben 2023 angekündigt, dass sie ab Anfang 2024 schrittweise damit beginnen, SPF/DKIM und DMARC aktiv einzufordern. Zunächst ist es so, dass Unternehmen, die E-Mails an Gmail- oder Yahoo-Konten senden, SPF oder DKIM nutzen müssen. Für Unternehmen, die mehr als 5.000 E-Mails pro Tag an Gmail oder Yahoo-Konten versenden sind die Anforderungen schon jetzt höher: Sie müssen SPF und DKIM unterstützen. Seit Einführung dieser Vorgaben im Februar 2024 haben einige Unternehmen bereits darüber geklagt, dass ihre E-Mails nicht mehr zugestellt werden. Sie mussten reagieren und die Vorgaben zu SPF und DKIM erfüllen. In den nächsten Monaten ist damit zu rechnen, dass Google und Yahoo die Vorgaben weiter hochschrauben werden. Es wird darauf hinauslaufen, dass Unternehmen dazu verpflichtet werden, SPF und DKIM ordentlich umzusetzen und einen korrekten DMARC-Eintrag zu setzen. Halten sich die Unternehmen nicht daran, werden ihre E-Mails nicht mehr an Gmail- und Yahoo-Konten zugestellt werden. Aus Datenschutz- und Sicherheitssicht ist diese Vorgehensweise begrüßenswert und es ist zu hoffen, dass auch die anderen E-Mail-Provider entsprechend nachziehen.

Warum ist ein aktives Monitoring sinnvoll?

Wie bereits erwähnt, senden empfangende E-Mail-Server täglich einen aggregierten Bericht an all jene E-Mail-Server, in deren Namen E-Mails eingegangen sind. Hierin sind sowohl die legitimen als auch die illegitimen E-Mails enthalten. Es empfiehlt sich, dass Organisationen diese Berichte auswerten, um die richtigen Schlüsse ziehen zu können. Hierfür gibt es auf dem Markt entsprechende Report-Analyse-Tools, die die Daten sauber aufbereiten. Die Verantwortlichen können damit sehr schön erkennen, von welchen Systemen aus gefälschte E-Mails (im Namen der eigenen Organisation) an welche Empfänger-Domains versendet wurden. Über die „abuse"-Benachrichtigung besteht die Möglichkeit, diese Fake-Sender zu stoppen. Außerdem hilft die Analyse insbesondere dabei, festzustellen, von welchen Systemen aus die Organisation E-Mails versendet. Damit kann auch frühzeitig erkannt werden, wenn es Zustellungsprobleme bei neu eingeführten Mailing-Systemen gibt und entsprechend reagiert werden. Sollten die E-Mail-Provider die Anforderungen weiter hoch setzen und die eigenen E-Mails nicht mehr zugestellt werden, ist dies ebenfalls sofort ersichtlich.

Über den Autor

Prof. Dr. Ronald Petrlic
ist Professor für Informationssicherheit an der TH Nürnberg. Er lehrt und forscht zu den Themen „Technischer Datenschutz", „E-Mail-Sicherheit" und „Decentralized Identities". Davor war er Leiter des Technik-Referats beim LfDI BaWü. Er berät Unternehmen zu technischen Fragestellungen im Datenschutz und bietet auch eine Monitoring-Lösung an. Nähere Informationen unter:

▶ www.datensicherheit.digital