

- **Landeskriminalamt
Mecklenburg-Vorpommern**

Email Sicherheit – SPF, DCIM und DMARC

Informationen und Handlungsempfehlungen des LKA MV
Vortrag, am 11.09.2024

LKA MV, Abteilung 7/ Digitales Service- und Kompetenzzentrum (DiSK)
KHK Jörg Patzer, 1. Sachbearbeiter Dezernat 74– Cybercrime + ZAC

Google und Yahoo – neue Anforderungen an Email Sicherheit

Ab April 2024 müssen E-Mail-Versender, die täglich mehr als 5.000 Nachrichten an Gmail-Konten senden, neue Anforderungen erfüllen, um eine reibungslose Zustellung ihrer E-Mails zu gewährleisten und zu verhindern, dass ihre Sendungen begrenzt oder als Spam markiert werden. Wir haben uns das einmal näher angesehen und daraus eine Anleitung erstellt, was Sie in Zukunft beachten müssen, um reibungsfrei mit Gmail Adressen kommunizieren zu können.

Grundlegende Anforderungen für alle Versender:

- Etablieren Sie SPF- und DKIM-E-Mail-Authentifizierung für Ihre Domain.
- Stellen Sie sicher, dass Ihre Versanddomains oder -IPs gültige Vorwärts- und Rückwärts-DNS-Einträge (PTR-Einträge) haben.
- Verwenden Sie eine TLS-Verbindung für den E-Mail-Verkehr.
- Halten Sie die Spam-Raten laut Postmaster-Tools unter 0,30 %

Quelle: <https://www.sentiguard.eu/wissen/google-verschaerft-seine-phishing-...>

Handlungsempfehlungen - E-Mail-Sicherheit

- → **Schutz vor Spoofing, Phishing und Fälschung**

SPF = Absenderadress-Fälschungen vermeiden

- Festlegung, welche Server im Namen der Domäne E-Mails versenden dürfen. Empfänger prüft Versandberechtigung des Absenders und kann so die E-Mails ablehnen.

DKIM = Sender-Authentifizierung

- Beim Empfang der E-Mail wird mittels Signatur erkannt, ob es sich um den korrekten Absender handelt und ob die E-Mail manipuliert wurde.

DMARC = Kontrollsystem

- Kontrollsystem mit Regelwerk, das über SPF und DKIM hinaus geht. Bsp. Reaktionen auf abgelehnte E-Mails sowie aktives Berichtswesen

Begriffsbestimmung SPF

- Vermeiden von Absender-Fälschungen mit **SPF (Sender Policy Framework)**
- (SPF) ist ein Sender-Authentifizierungs Verfahren (SENDER == Mailserver)
- Erkennung einer E-Mail, welche von einem nicht zum Versand autorisierten E-Mail Server gesendet wurde
- Die Fälschung des Absenders wird gern bei SPAM, Phishing oder CEO Fraud genutzt
- Email Server die nicht zum Versand im Namen einer Domain berechtigt sind, werden so erkannt
- **Wie macht man das?**
- Anlegen eines speziellen TXT Ressource Record Eintrag in der DNS-Zone einer Domain
- Eintrag enthält Informationen, welche E-Mail Server im Namen **IHRER** Domain Emails versenden dürfen
- Führt der Empfänger beim Eingehen einer E-Mail die SPF Prüfung durch, kann er feststellen, in wie weit der versendende Server die Versandrechte für **IHRE** Absender-Domain besitzt
- Ist ein E-Mail Server nicht im Domain SPF Eintrag benannt, so kann der empfangende E-Mail Server diese Mail ablehnen oder in Quarantäne verschieben

Schaubild

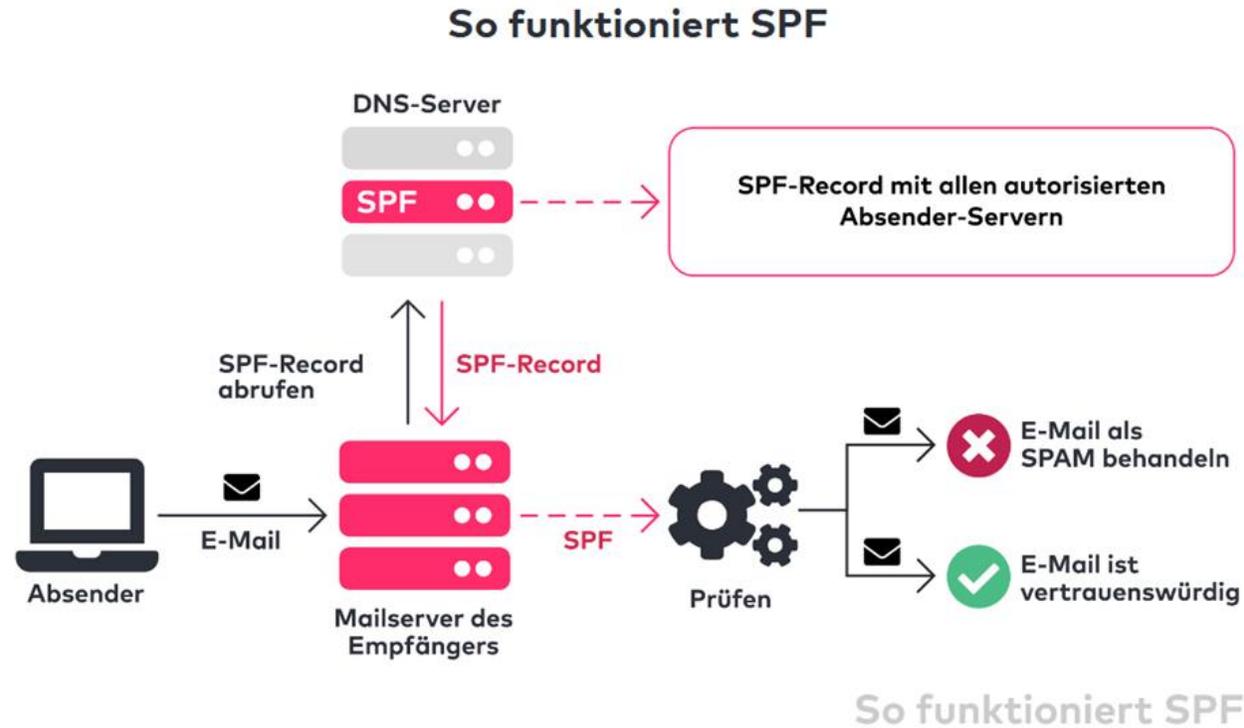


Abbildung: Wie funktioniert ein SPF-Record?

Absender: Sendet eine E-Mail

Mailserver des Empfängers: Entnimmt den Domainnamen aus der Absender-E-Mail-Adresse

SPF - abrufen: Anhand des Domainnamens den SPF-Record abrufen

DNS-Server: Liefert den TXT-Record in dem der SPF-Record eingetragen ist

Prüfen ob die IP-Adresse des Absenders der E-Mail durch den SPF-Record autorisiert ist, E-Mails zu senden

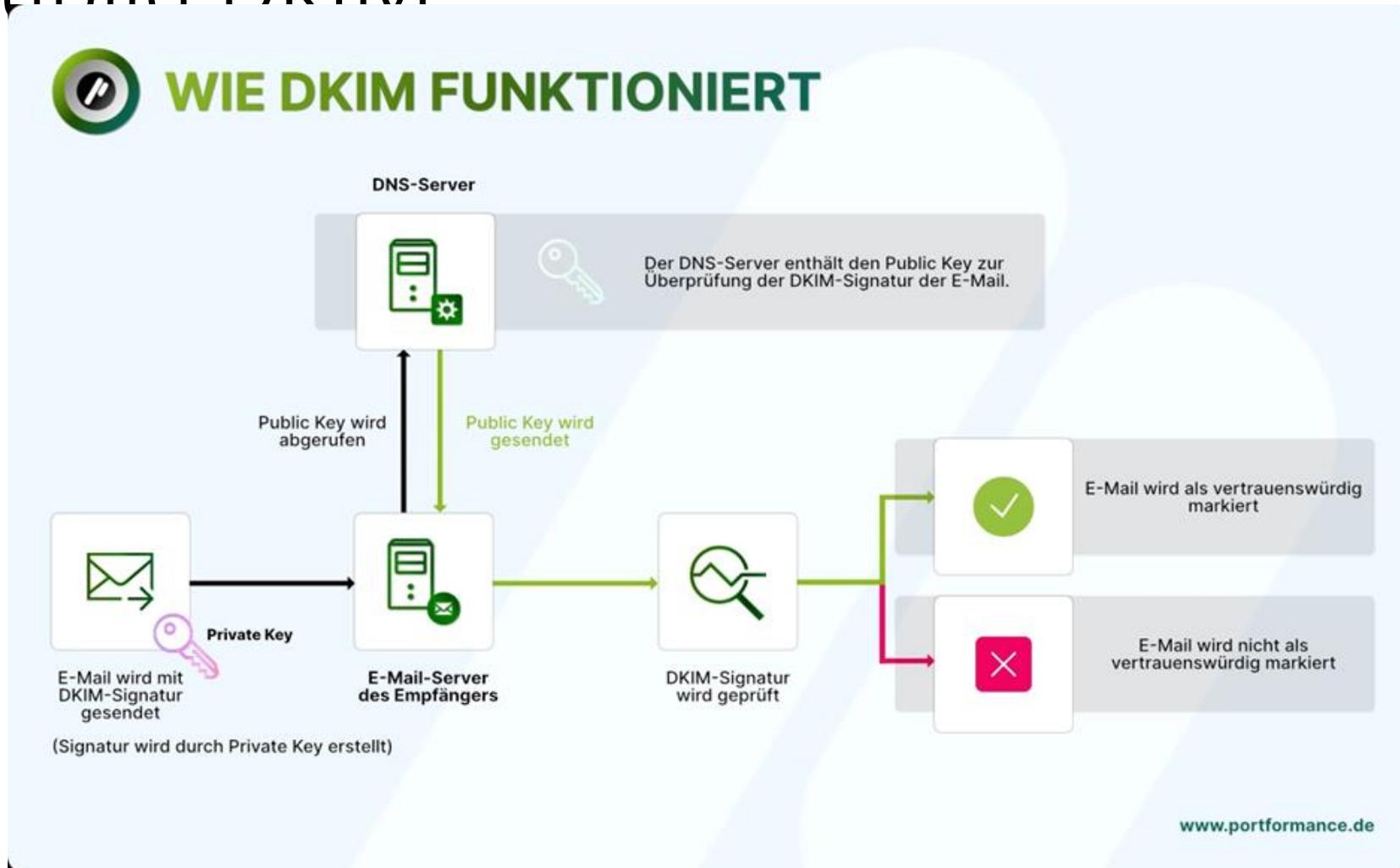
- **E-Mail als SPAM Behandeln**

- **E-Mail ist vertrauenswürdig**

Begriffsbestimmung DKIM

- DomainKeys Identified Mail (DKIM) bildet neben SPF einen weiteren Sicherheitsschritt für IHREN E-Mail-Verkehr
- Es ist wie ein digitaler Fingerabdruck für IHRE E-Mails
- Es sorgt dafür, dass der Inhalt IHRER E-Mail unterwegs nicht verändert wurde und bestätigt, dass sie wirklich von IHRER Domain stammt
- DKIM hilft dir, das Vertrauen in IHRE E-Mail-Kommunikation zu stärken
- Es stellt sicher, dass IHRE Nachrichten unterwegs nicht manipuliert werden
- Erhöht die Wahrscheinlichkeit, dass IHRE E-Mails nicht als Spam eingestuft werden
- Ein gut konfigurierter DKIM-Eintrag ist ein unverzichtbarer Teil IHRER E-Mail-Sicherheitsstrategie

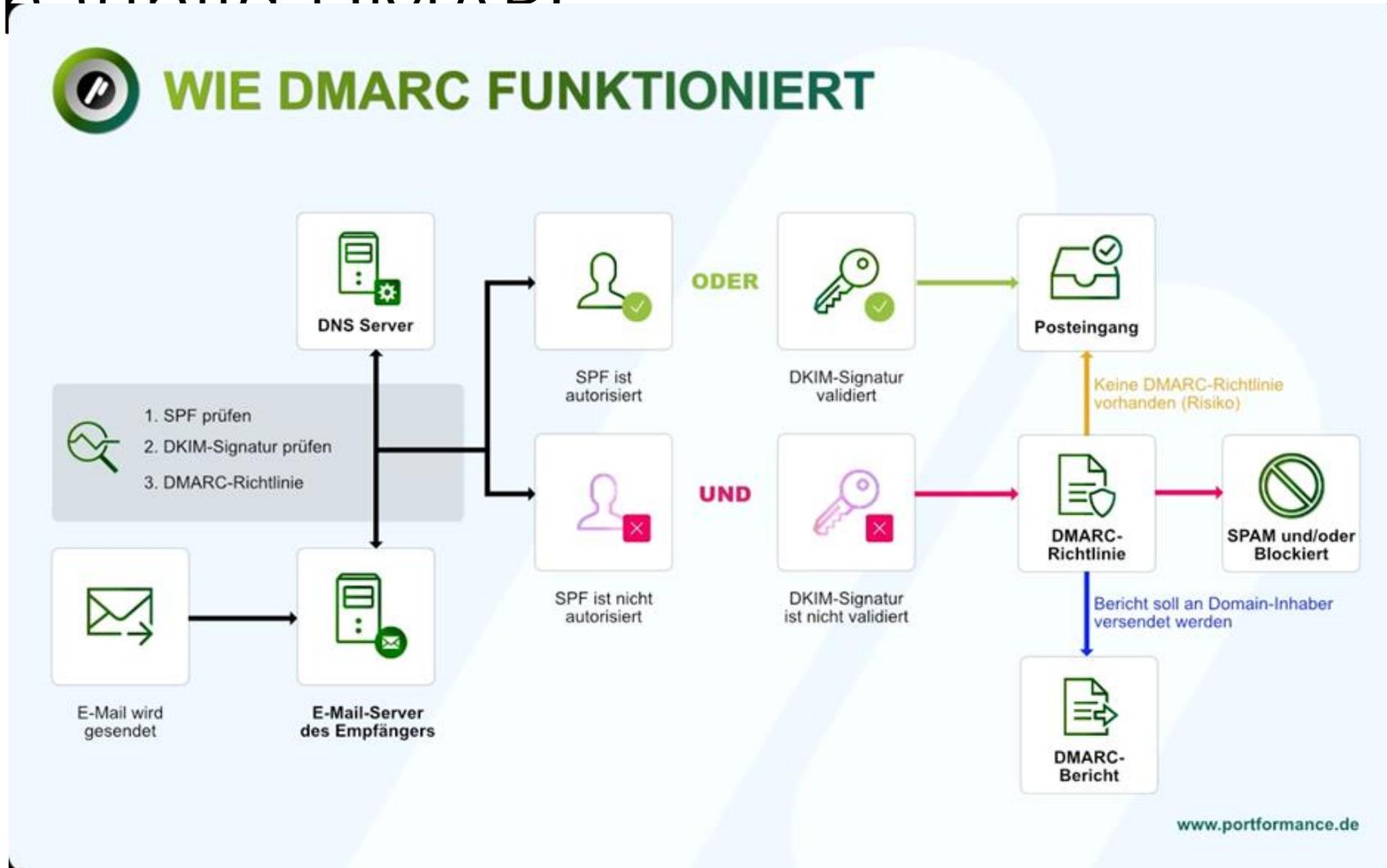
Schaubild DKIM



Begriffsbestimmung DMARC

- Kontrollsystem **DMARC (Domain-based Message Authentication, Reporting and Conformance)**
- DMARC ist ein auf einem Regelwerk basierendes Kontrollsystem
- Ein DMARC-Eintrag sagt dem Empfänger E-Mail Server, ob er die E-Mail bei fehlerhafter Prüfung auf SPF und/oder DKIM annehmen soll oder nicht
- Er fungiert als virtueller Sicherheitsbeauftragter für IHRE eigene Domain.
- E-Mails, welche durch die SPF bzw. DKIM Prüfung beim empfangenden E-Mail Server durchgefallen sind, werden entsprechend der Anweisungen des DMARC Eintrages gelöscht, zurückgewiesen oder in dem Spam-Ordner verschoben
- Der Empfänger der E-Mail kann dem Domaininhaber über den Missbrauch und Probleme mit der Authentifizierung durch Versand eines Berichtes an eine bei IHNEN im DMARC Eintrag festgelegte E-Mail Adresse aktiv informieren
- Mit Nutzung eines DMARC Eintrages in seiner DNS-Zone, kann der Domaininhaber wichtige Informationen erlangen
- wer versucht E-Mails im Namen des Domaininhabers zu versenden (aktive Meldung von Spoofing Versuchen)

Schaubild DMARC



Mail Sicherheit - Fazit

Warum sollten Sie SPF, DKIM und DMARC verwenden?

Die Authentifizierungsmethoden SPF und DKIM zählen zu den Schlüsselpunkten zur Optimierung Ihrer Zustellbarkeit und hat sich zum Standard in der E-Mail-Welt entwickelt.

Aber das ist nicht der einzige Vorteil.

Tatsächlich verbessert die Implementierung dieser Protokolle die Zustellbarkeit von E-Mails. Dank dieser Methoden werden IHRE E-Mails besser von ISPs (Internet Service Providern) und den E-Mail-Clienten Ihrer Empfänger identifiziert.

Diese Protokolle dienen zur Überprüfung der Identität von Absendern und zählen zu den effektivsten Möglichkeiten, um zu verhindern, dass Phisher (Betrügerische E-Mails mit dem Ziel sensible Daten wie Kundenlogin, Bankverbindungen etc. zu erbeuten) und andere Betrüger sich als legitimer Absender ausgeben, dessen Identität sie unter demselben Domainnamen angeben könnten.

Vielen Dank für Ihre Aufmerksamkeit

- **Ansprechpartner/ Rückfragen:**
 - **Landeskriminalamt Mecklenburg-Vorpommern**
 - **KHK Jörg Patzer, 1. Sachbearbeiter Dezernat 74/ Cybercrime und Mitglied der ZAC**
 - **Hotline ZAC: 03866 / 64 – 9494**
 - **E-Mail: zac@lka-mv.de**
- **<https://polizei.mvnet.de/Polizei/LKA>**