Sicherer E-Mail-Verkehr im Unternehmensumfeld

– Schutz vor Bedrohungen und Sicherung der Geschäftskontinuität –

WIR GESTALTEN DAS INTERNET.
GESTERN. HEUTE. ÜBER MORGEN.

eco
VERBAND DER INTERNETWIRTSCHAFT

E-Mails sind unverzichtbar und Grundlage Ihren Geschäftskommunikation. Lassen Sie uns entdecken, wie wir E-Mails schützen und gleichzeitig das Geschäft stärken können.

Michael Weirich,
eco – Verband der Internetwirtschaft e.V.

Lichtstraße 43h
50825 Köln

Fon +49 (0) 221 – 7000 48-193

michael.weirich@eco.de
https://www.eco.de

André Görmer,
Senior Director Solutions&Services
Mapp Digital GmbH
[Leiter der eco Kompetenzgruppe E-Mail]

Fon +49 (0) 176 – 12009-762

andre.goerme@mapp.de
https://www.mapp.de

Bei Fragen wenden Sie sich gerne an uns: e-mail@eco.de

E-Mail im Unternehmensumfeld

- E-Mail gibt es seit mehr als 50 Jahren.
- 1984 wurde in Deutschland die erste E-Mail empfangen.
- Im Schnitt erhalten die Deutschen 26 berufliche E-Mails pro Tag.
- Ältere erhalten mehr E-Mails als Jüngere.
  - 50- bis 64-Jährige Berufstätige: erhalten durchschnittlich 30 E-Mails pro Tag.
  - 30- bis 49-Jährige Berufstätige: erhalten durchschnittlich 26 E-Mails pro Tag.
  - 16- bis 29-Jährige Berufstätige: erhalten durchschnittlich 22 E-Mails pro Tag.

E-Mail im Unternehmensumfeld

E-Mail bleibt ein zentrales Kommunikationsmittel

Besonders geeignet für präzise und wichtige Informationen.
Wichtige Entscheidungen und Zusammenfassungen werden bevorzugt per E-Mail versendet.

Weitere verbreitete Kommunikationsmittel

Messenger:
Ideal für schnelle Absprachen, die nachverfolgt werden sollen.
Video Konferenzen:
Wird für Videotelefonie und virtuelle Meetings verwendet.
Telefon:
Kommt zum Einsatz, wenn sofortige Antworten benötigt werden.

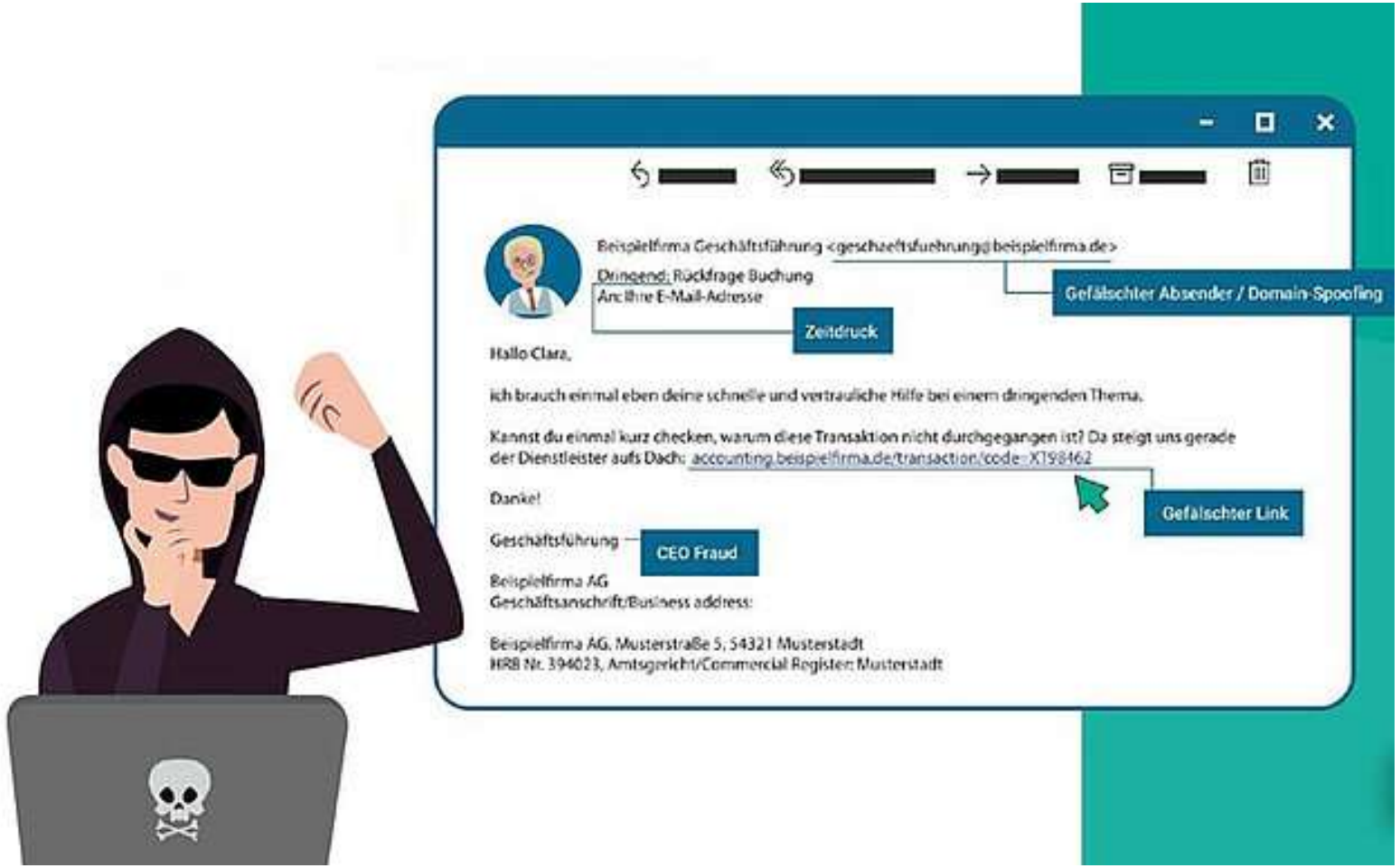
Warum ist E-Mail-Sicherheit wichtig

- Mensch als Hauptangriffspunkt: Laut Untersuchungen der größte Risikofaktor für die Sicherheit von IT-Systemen in Behörden und Unternehmen.
- Phishing als Hauptangriffsmethode: **92%** aller Cyberangriffe beginnen mit einer Phishing-Mail.
- Hohe Klickrate bei Phishing-Mails: Fast **75%** der Nutzer klicken auf mindestens eine von drei Phishing-Mails.

Warum ist E-Mail-Sicherheit wichtig

- Vertraulichkeit und Datenschutz
  Schutz sensibler Informationen
  Einhaltung gesetzlicher Vorschriften
- Integrität der Kommunikation
  Verhindern von Datenmanipulation
  Vermeidung von Identitätsdiebstahl
- Geschäftskontinuität und Reputation
  Verhindern von Datenmanipulation
  Vermeidung von Identitätsdiebstahl
- Schutz vor unbefugtem Zugriff
  Verhindern von Spionage
  Sicherung der Kommunikation

Bedrohungen für E-Mail-Sicherheit



Erläuterungen zu einer Phishingmail (Abbildung: SoSafe GmbH)

Bedrohungen für E-Mail-Sicherheit

- Phishing: Betrügerische E-Mails, die vertrauliche Informationen stehlen wollen.
- Malware wird oft über E-Mail-Anhänge oder Links in E-Mails verbreitet.
- Spoofing: Fälschung von E-Mail-Absenderadressen, um Vertrauen zu gewinnen.

Sichere E-Mail - jetzt -

- Sichere E-Mail ist eine Grundlage Ihres Geschäftserfolges
- Zusammen mit dem **Bundesamt für Sicherheit in der Informationstechnologie** (BSI) setzt sich eco für sichere E-Mail im Unternehmensumfeld ein.
- Die Kompetenzgruppe E-Mail gibt Hilfestellungen und Anleitungen, um auch in Ihrem Unternehmen sichere E-Mail zu realisieren.
- https://www.eco.de/sichere-e-mail

INITIATIVE SICHERE E-MAIL

Die Certified Senders Alliance (CSA)

Die CSA zertifiziert Versender von kommerziellen E-Mails, die hohe Qualitätsstandards einhalten. Mit der CSA-Zertifizierung erhalten Sie Zustellbarkeitsvorteile bei internationalen Mailbox- und Spamfilter

- Im Certification Monitor erhalten CSA Versender Einblicke in Deliverability KPIs, um bspw. Kunden zu identifizieren, die ihrer Reputation schaden.

- Monitoring und Auswertung von:
  Spam Trap Hits
  DKIM Errors
  Spam Complaint Rate

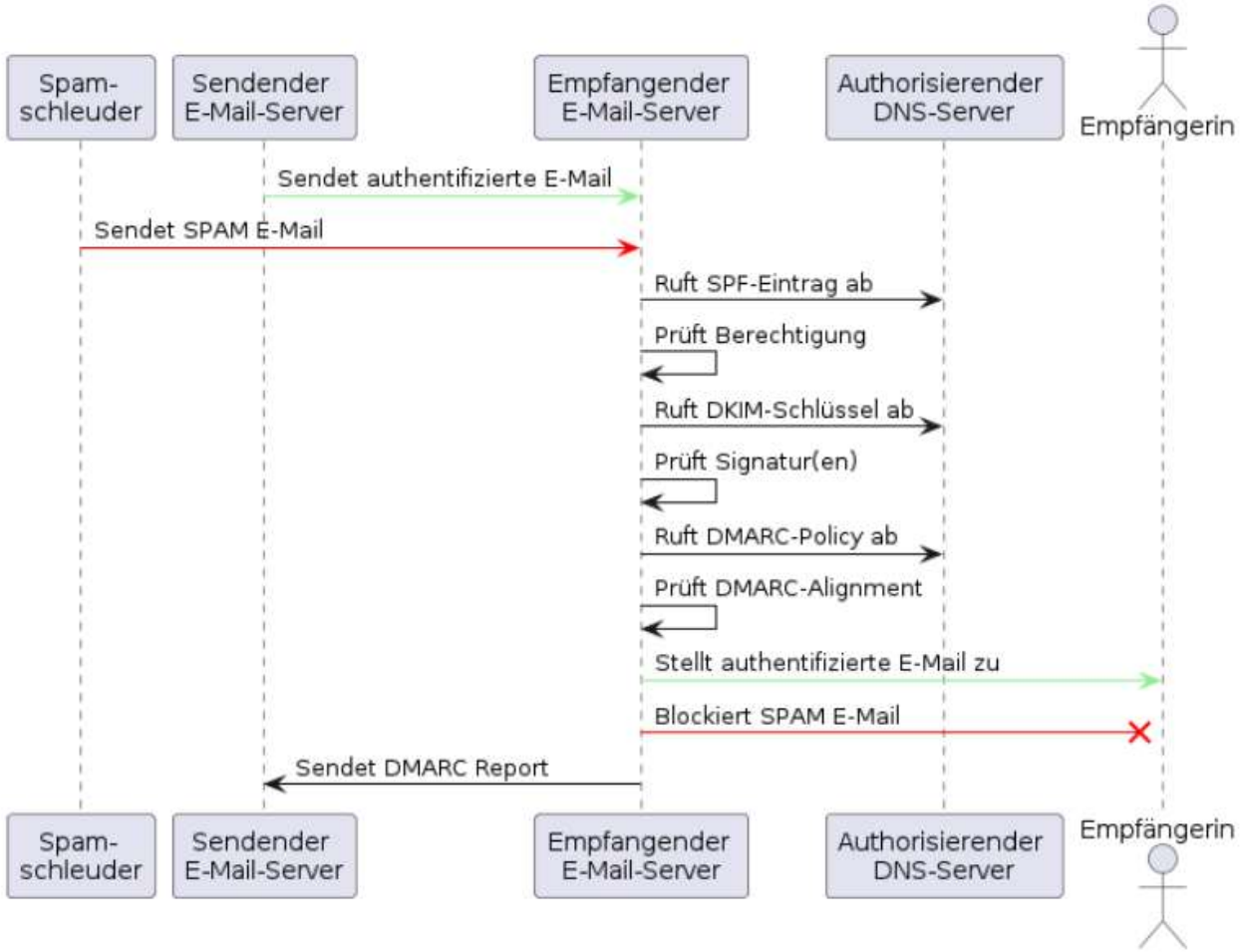
https://certified-senders.org/

sichere E-Mail - die Grundlagen -

- **SPF (Sender Policy Framework)**: Überprüft, ob eine E-Mail von einem autorisierten Server gesendet wurde. (RFC 7208)
- **DKIM (DomainKeys Identified Mail)**: Fügt digitale Signaturen zu E-Mails hinzu, um ihre Authentizität zu bestätigen. (RFC 6376, RFC 8463)
- **DMARC (Domain-based Message Authentication, Reporting & Conformance)**: Kombiniert SPF und DKIM und fügt Berichterstattung hinzu, um E-Mail-Spoofing zu verhindern. (RFC 7489)

sichere E-Mail-Kommunikation

Ablauf einer Authentifizierung mit SPF, DKIM und DMARC.



sichere E-Mail-Kommunikation
- weitere Schritte -

- **DNS-Based Authentication of Named Entities (DANE/TLSA)**: (RFC 7671)

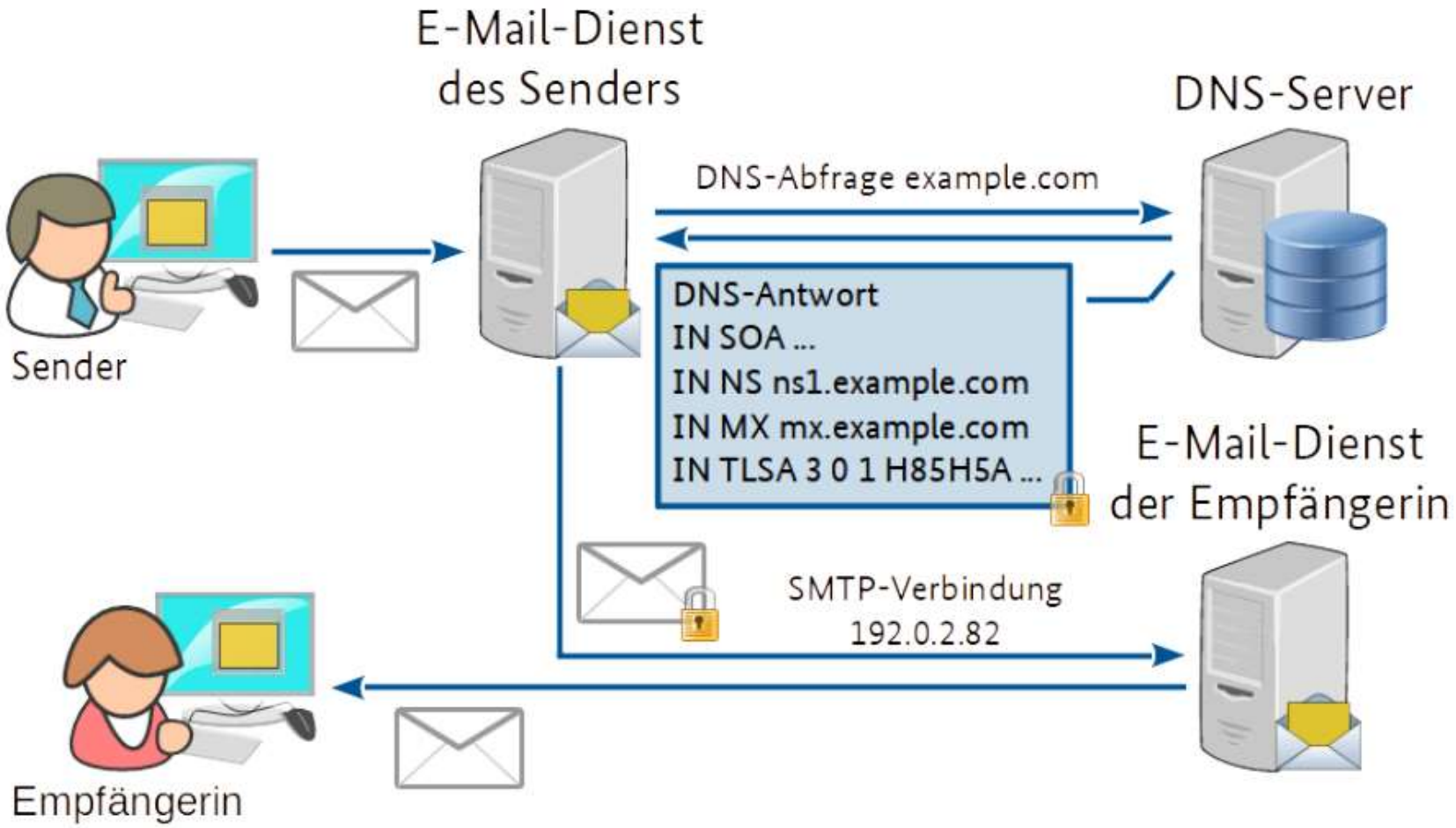
Zeigt E-Mail-Dienst des Senders an, dass STARTTLS gefordert wird.
Fingerprint des für die TLS-Verbindung genutzten Zertifikats im TLSA-Eintrag.

- **DNS Security Extension (DNSSEC)**: (RFC 6781, RFC 4033)

Sichert DNS-Einträge vor Manipulation.
Voraussetzung für DANE/TLSA.

Lösungen für sichere E-Mail-Kommunikation - DANE

Funktionsweise DANE/TLSA.



Lösungen für sichere E-Mail-Kommunikation - Zertifikate

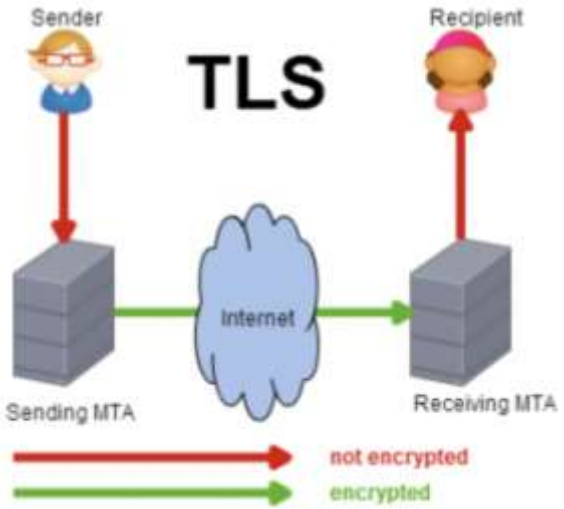
Signaturen und Verschlüsselung.

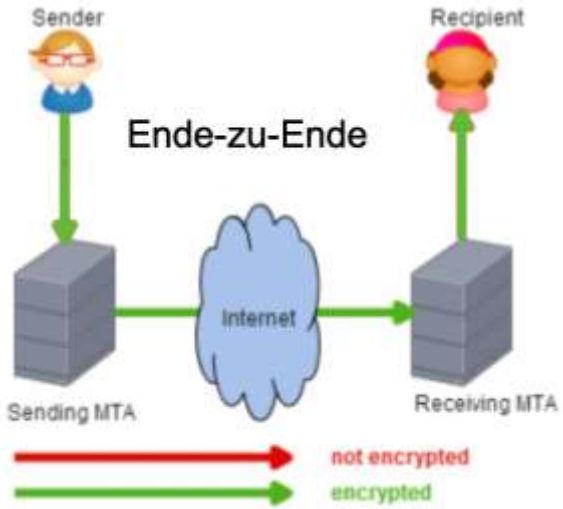
S/MIME (Secure/Multipurpose Internet Mail Extensions) -
Ein Standard für die Verschlüsselung und digitale Signatur von E-Mails.

- Mittels S/MIME kann seitens des Empfängers die Identität des Absenders verifiziert werden.
- Sicherstellen der Vertraulichkeit, Integrität und Authentizität einer Mail.
- Vertrauensvolle E-Mail-Kommunikation stärkt das Vertrauen und schützt sensible Informationen.
- Transport Layer Security (TLS): Verschlüsselt die Übertragung von E-Mails zwischen Servern.

Lösungen für sichere E-Mail-Kommunikation - End2End vs TLS -

Ende zu Ende vs. Transport Verschlüsselung.



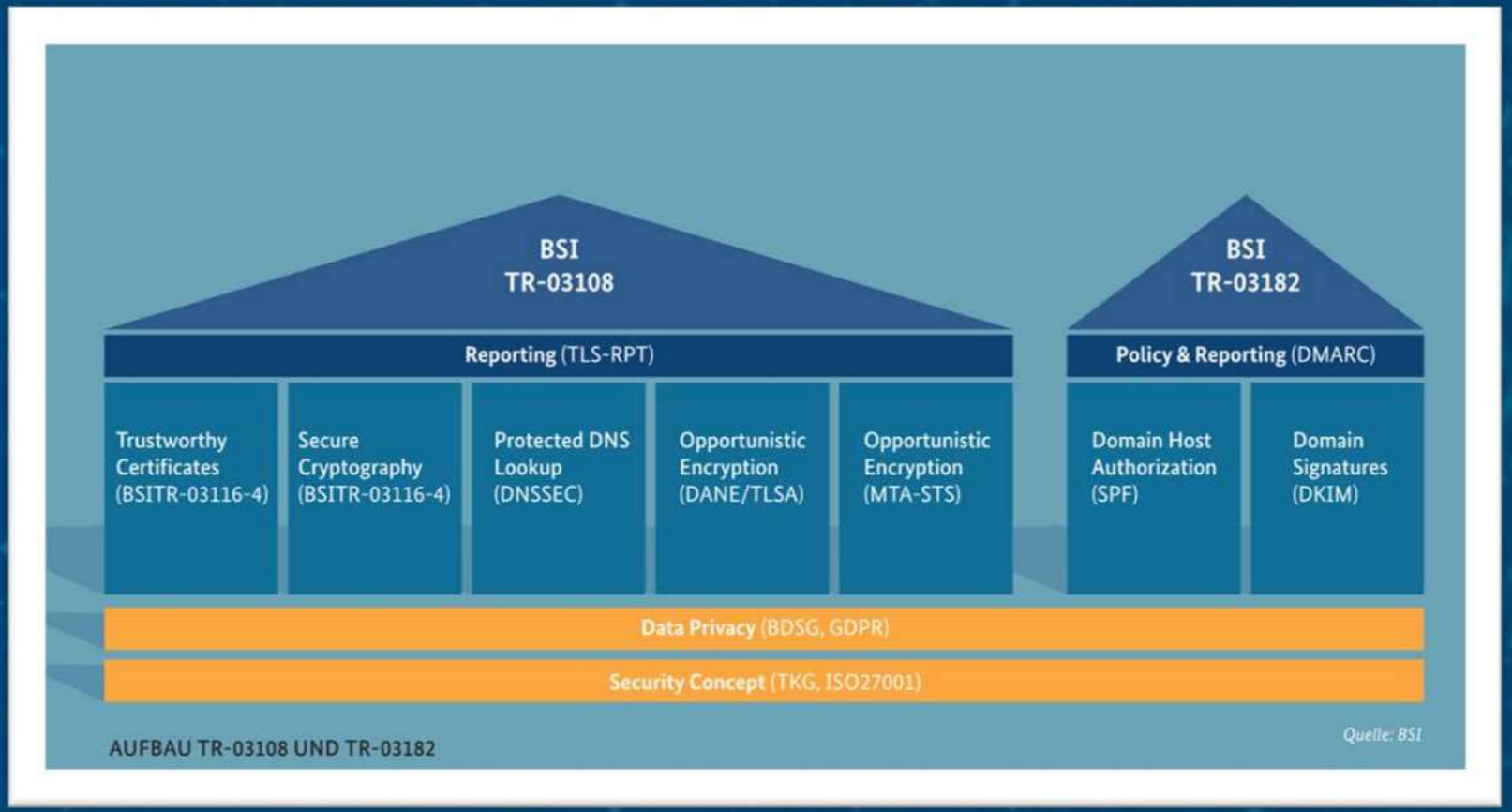


- Transport Layer Security (TLS): Verschlüsselt die Übertragung von E-Mails zwischen Servern.
- Ende-zu-Ende (z.B. PGP oder S/MIME) verschlüsselt die Mail auf dem Gesamten Weg

Lösungen für sichere E-Mail-Kommunikation

BSI TR-03108 und BSI TR-03182

Anforderungen des BSI und europäischer Partnerbehörden



AUFBAU TR-03108 UND TR-03182

- Informeller Austausch in MESSEU-Workshops unter Beteiligung von EU Institutionen (JRC)
- Anforderungen der Partnerbehörden sind weitestgehend identisch
- Und sind Teil der Cybersecurity Strategy for the Digital Decade der EU Kommission

Effektive E-Mail-Sicherheitsstrategien

- **SPF zur Unterstützung der Geschäftskontinuität**:

Durch die Überprüfung, ob E-Mails von autorisierten Servern gesendet werden, reduziert SPF das Risiko von Phishing-Angriffen. Dies verringert Ausfallzeiten, die durch Cyberangriffe entstehen, und trägt so zur Stabilität des Geschäftsbetriebs bei.

- **DKIM und Domain-Reputation**:

DKIM verbessert die Domain-Reputation, indem es sicherstellt, dass E-Mails digital signiert sind und deren Authentizität bestätigt wird. Dies verhindert, dass legitime E-Mails als Spam markiert oder blockiert werden, was die Kommunikationseffizienz und den Geschäftserfolg unterstützt.

Effektive E-Mail-Sicherheitsstrategien

- **DMARC für proaktiven Markenschutz**:

Mit DMARC können Unternehmen Berichte über E-Mail-Missbrauch erhalten und so proaktiv handeln, um Spoofing und Angriffe auf ihre Marke zu verhindern. Dies stärkt das Vertrauen in die Marke und schützt die Integrität des Unternehmens.

- **DNSSEC und DANE für Vertrauen bei Kunden und Partnern**:

Diese Technologien helfen, die Sicherheit der Kommunikation zu gewährleisten, indem sie Manipulationen verhindern. Dies stärkt das Vertrauen von Kunden und Geschäftspartnern und fördert langfristige Beziehungen durch sichere und authentifizierte Kommunikation.

Key Takeaways: Maßnahmen

- **SPF, DKIM und DMARC implementieren**:

IT-Infrastruktur:
Setzen Sie SPF, DKIM und DMARC auf, um den E-Mail-Verkehr zu authentifizieren und Phishing-Angriffe sowie E-Mail-Spoofing zu verhindern.

Management:
Schulen Sie Mitarbeiter über die Bedeutung dieser Protokolle und kommunizieren Sie die Vorteile, wie den Schutz der Unternehmensmarke und die Verringerung von Cyberangriffen

Key Takeaways: Maßnahmen

- **Überprüfung und Optimierung der bestehenden DNS-Sicherheit**:

IT-Infrastruktur:
Führen Sie DNSSEC und DANE ein, um Manipulationen und Man-in-the-Middle-Angriffe auf die DNS-Infrastruktur zu verhindern.

Management:
Stellen Sie sicher, dass diese Sicherheitsmaßnahmen Teil der Unternehmensrichtlinien werden, um Vertrauen bei Kunden und Partnern zu stärken.

Key Takeaways: Maßnahmen

- **Proaktive Überwachung und Reporting**:

IT-Infrastruktur:
Aktivieren Sie Berichtsmechanismen über DMARC, um Missbrauch frühzeitig zu erkennen und darauf zu reagieren.

Management:
Nutzen Sie diese Berichte, um strategische Entscheidungen zu treffen und präventiv auf potenzielle Bedrohungen zu reagieren.

Sichere Kommunikation ist wie guter Kaffee – man merkt erst, wie wichtig sie ist, wenn sie fehlt.

Danke für Ihre Aufmerksamkeit und auf eine sichere Zusammenarbeit… und hoffentlich immer genug Kaffee im Büro!

Bei Fragen wenden Sie sich gerne an uns: e-mail@eco.de