ENCRYPTION

E-Mails im Business.

Sicher und DSGVO-konform E-Mails versenden

digicert®

InterNetX

Inhaltsverzeichnis.

EXECUTIVE SUMMARY 03

E-MAILS IM BUSINESS 04

KAPITEL 01
MAILINGS & ALLES, WAS „RECHT" IST: GESETZLICHE VORGABEN 06

KAPITEL 02
ENCRYPTION – NUR FÜR IT-FIRMEN? 08

KAPITEL 03
BEST PRACTICE E-MAIL-VERSCHLÜSSELUNG FÜR UNTERNEHMEN 16

ENCRYPTION: CHANCE UND LÖSUNG 21

QUELLENANGABEN & BILDNACHWEIS 22

ABOUT 23

EINLEITUNG
KAPITEL 01
KAPITEL 02
KAPITEL 03
FAZIT

Executive Summary.

Alle haben sie mehr oder weniger in den letzten Jahren gespürt: die Auswirkungen der EU Datenschutz-Grundverordnung (DSGVO) im Unternehmen. Sie hat in vielen Bereichen für Veränderungen gesorgt und bleibt eine der Triebkräfte der Digitalisierungsprozesse.

Der Versand von E-Mails und die damit verbundenen technischen und juristischen Vorgaben bleiben häufig weiterhin unsicheres Terrain. Zum einem sind die Normen nicht bekannt oder sie lassen Interpretationsspielraum hinsichtlich technischer Schutzmaßnahmen. Zum anderen ist vielen Unternehmen oft auch die Dringlichkeit einer Inhalts- und Transportverschlüsselung von E-Mails in ihrem eigenen Segment nicht bewusst. Sicher aber bleibt: Bei Rechtsverstößen drohen den E-Mail-Versendern nicht nur immense Reputationsschäden, sondern auch Bußgelder.

Für einen DSGVO-konformen E-Mail-Versand braucht es:

- Interne Compliance-Vorgaben
- Strategische Entscheidungen über Security-Dimensionen
- Maßnahmen zur Implementierung

Dieses E-Paper klärt über die notwendigen Maßnahmen für den DSGVO-konformen E-Mail-Versand auf und stellt technische Lösungswege vor. Am Ende findet sich ein Best-Practise-Szenario, um Unternehmen zu unterstützen, sich darauf einzustellen.

Ziel ist es, eine allgemeine Sensibilisierung für das Thema datenschutzkonformer E-Mail-Versand herzustellen. Das E-Paper wurde daher nach bestem Wissen und Gewissen erstellt, erhebt allerdings keinen Anspruch auf Vollständigkeit bzw. Richtigkeit und es kann weder auf unternehmensspezifische Besonderheiten eingehen noch eine individuelle Rechtsberatung ersetzen.

EINLEITUNG
KAPITEL 01
KAPITEL 02
KAPITEL 03
FAZIT

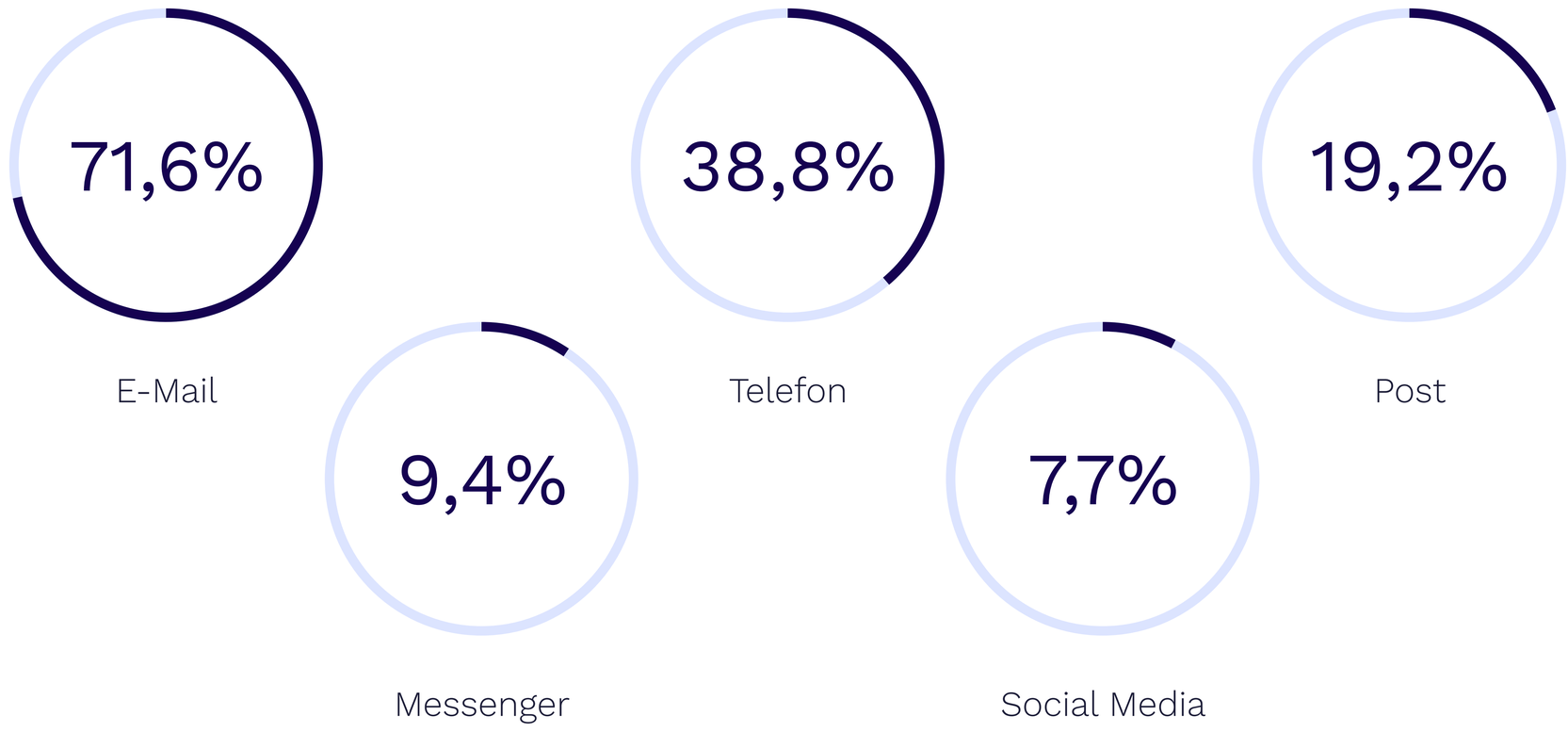
E-Mails im Business.

Phishing-Attacken boomen und immer häufiger kommt es zum Missbrauch von (Online-)Identitäten und E-Mails. Durch diverse Datenskandale der letzten Jahre sollte klar sein, dass Information im Netz systematisch überwacht und abgegriffen werden. Dazu zählen auch Daten in Unternehmen. Datenschützer fordern zu Recht höhere Standards, vor allem beim E-Mail-Versand.

Nicht umsonst werden E-Mails oft mit digitalen Postkarten verglichen. Wer sie transportiert, kann sie lesen – zumindest, wenn keine weiteren Schutzmaßnahmen ergriffen werden. Ohne zusätzlichen Schutz sind Daten im Netz leicht für Dritte zugänglich. Der Zugriff auf Kunden- bzw. Mitarbeiterdaten, auf das neueste Projekt in der Entwicklungsabteilung oder auf das interne Sicherheitssystem kann Unternehmen, egal welcher Größe, empfindlich treffen.

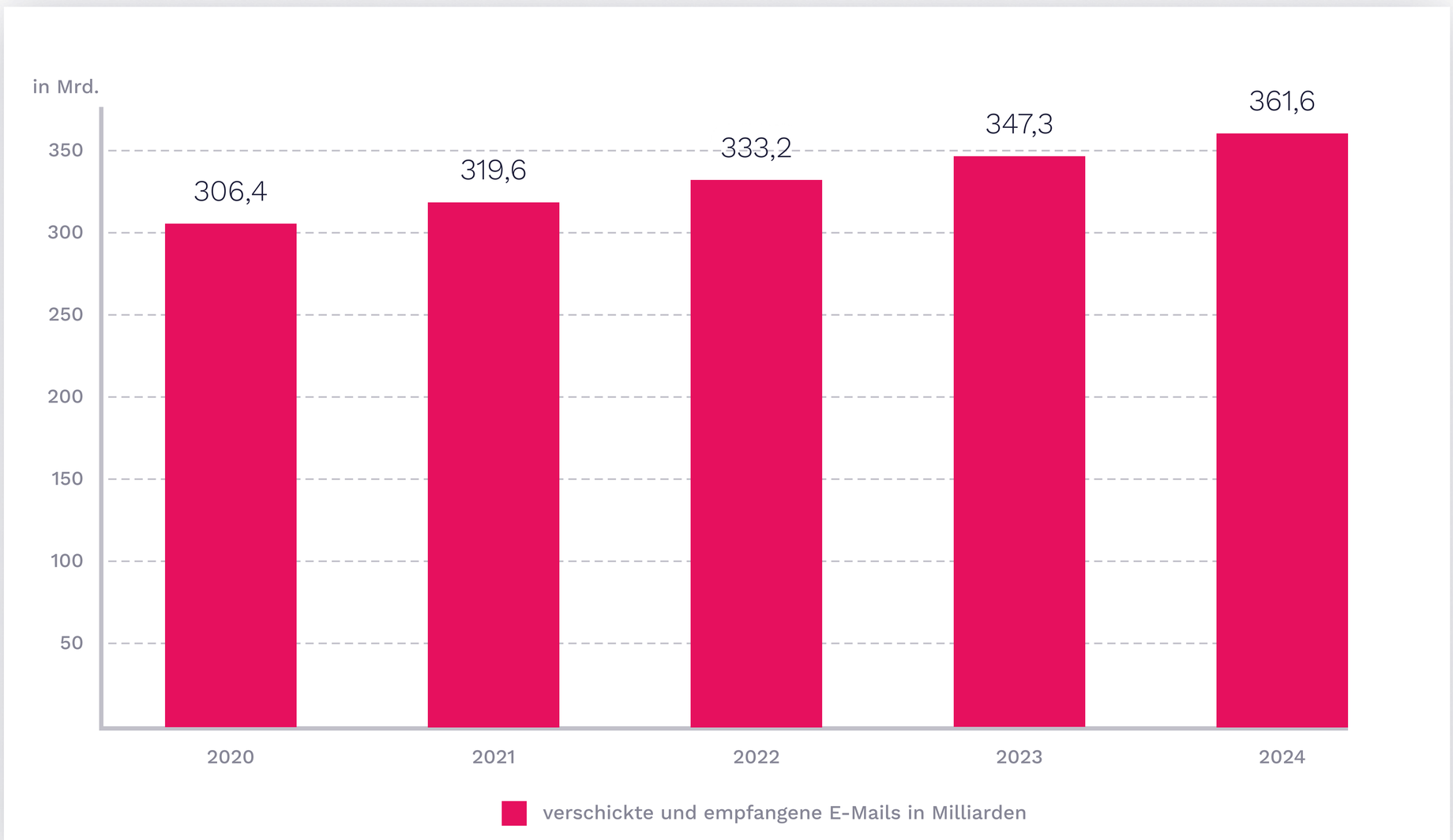
Vor allem im Zuge von COVID-19 hatten diese Entwicklungen einschneidende Auswirkungen auf Wirtschaft, Datenverarbeitung und Kommunikation. Online-Meeting-Tools, Chats und insbesondere die “klassische” E-Mail haben sich als zentrale Medien im geschäftlichen Umfeld herausgestellt.

VERBRAUCHER KOMMUNIZIEREN MIT UNTERNEHMEN VIA:



Studie Deutschland Digital 2020 im Auftrag von WEB.DE und GMX
(Repräsentative Studie der Convios Consulting GmbH)

Das zeigt auch diese Prognose, nach welcher der E-Mail-Versand bis 2024 um 18% zunehmen wird:



Prognose zur Anzahl (in Milliarden) der täglich versendeten und empfangenen E-Mails weltweit von 2020 bis 2024 © Statista 2021

Unternehmen geben in E-Mails Daten aller Art weiter: Das reicht von der einfachen Notiz bis hin zu personenbezogenen Daten und wirtschaftlich relevanten Interna. Speziell dieser Kommunikationskanal erweist sich daher als besonders zentral und auch schützenswert – vor allem hinsichtlich der DSGVO.

Unternehmen verspüren im Zuge der beschleunigten Digitalisierung sowie den damit einhergehenden rechtlichen Anforderungen häufig Unsicherheiten: Reichen die getroffenen Schutzmaßnahmen aus? Sind Unternehmen über die rechtlichen Anforderungen und Risiken hinreichend informiert?

EINLEITUNG
KAPITEL 01
KAPITEL 02
KAPITEL 03
FAZIT

Mailings & alles, was „Recht" ist: gesetzliche Vorgaben.

Mit Einführung der DSGVO wurden die Rechte der EU-Bürger:innen an ihren eigenen Daten gestärkt, indem verpflichtende Grundsätze für die Verarbeitung personenbezogener Daten aufgestellt wurden. Jede Datenverarbeitung muss nun auf einer konkreten Rechtsgrundlage beruhen. Die wichtigsten Rechtsgrundlagen wurden in Art. 6 Abs. 1 DSGVO normiert. Danach kann die Datenverarbeitung entweder durch eine Einwilligung des Betroffenen legitimiert oder auf einen gesetzlichen Ermächtigungsgrund (wie z. B. Erforderlichkeit für die Erfüllung eines Vertrages) gestützt werden.

> **Artikel 32 der Verordnung** legt explizit fest, dass Verantwortliche geeignete technische Maßnahmen zum Schutz personenbezogener Daten durchführen müssen, wie etwa die Pseudonymisierung und Verschlüsselung. Verstöße gegen die DSGVO haben teils empfindliche Bußgelder zur Folge.

Unabhängig von der Rechtsgrundlage folgt aus dem **Grundsatz der Integrität und Vertraulichkeit**, dass bei der Datenverarbeitung eine angemessene Sicherheit zu gewährleisten ist, die u.a. einen **Schutz vor unbefugter oder unrechtmäßiger Verarbeitung** durch geeignete technische und organisatorische Maßnahmen vorsieht, welche wiederum durch **Art. 32 DSGVO** konkretisiert werden.

Das **Bundesdatenschutzgesetz (BDSG)** ergänzt und konkretisiert die Vorgaben der DSGVO für Deutschland und gibt einen streng geregelten Rahmen für den Umgang mit personenbezogenen Daten vor.

Mit dem **Gesetz zur Kontrolle und Transparenz im Unternehmens-bereich (KonTraG)** wurde bereits 1998 eingeführt, dass Maßnahmen zu treffen sind, welche unternehmerische Risiken früh erkennen und nach Möglichkeit auf ein tragbares Maß begrenzen. Zu den Maßnahmen, zählen (meist im Rahmen von Schutzkonzepten) nach heutigem Stand der Technik längst u.a.:

- **Firewalls** als Barriere zwischen den Netzwerken
- **Signaturen** zur Identitätsprüfung
- **Encryption**, um die Vertraulichkeit von Inhalten sicherzustellen

EINLEITUNG
KAPITEL 01
KAPITEL 02
KAPITEL 03
FAZIT

DSGVO oder GDPR

Im Zusammenhang mit der DSGVO fällt oft der Begriff GDPR. Er steht für “General Data Protection Regulation”. Es handelt sich dabei um den internationalen Ausdruck für “Datenschutzgrundverordnung”, also um die englische Entsprechung zu DSGVO.

Gesetzeskonforme E-Mail-Kommunikation stellt also nicht nur eine Notwendigkeit dar, um Strafen zu entgehen. Sie kann vielmehr als entscheidender Wettbewerbsfaktor genutzt werden:

Kunden und Partner achten mehr denn je darauf, was mit ihren Daten geschieht und wie mit ihnen umgegangen wird. Im Zweifel wählen sie den Anbieter, der ihnen durch eine verschlüsselte Kommunikation mehr Sicherheit bietet.

Verschlüsselung

(oder Encryption, Kryptographie) Klartext bzw. Daten werden hierbei mit einem Schlüssel codiert. Diese so codierte Zeichenfolge lässt sich nur mit dem passenden Schlüssel decodieren.

Die DSGVO gilt nicht nur für alle Unternehmen, die ihren Sitz in der EU haben, sondern auch für außereuropäische Firmen, die auf dem europäischen Markt tätig sind oder personenbezogene Daten von EU-Bürgern verarbeiten.

EINLEITUNG
KAPITEL 01
KAPITEL 02
KAPITEL 03
FAZIT

Encryption – nur für IT-Firmen?

Hier lässt sich definitiv sagen: Nein. Alle Unternehmen, die digitalen Schriftverkehr pflegen, sehen sich zunehmend mit Gefährdungen aus dem Netz sowie neuen rechtlichen und technischen Vorgaben konfrontiert. Wer davon ausgeht, dass dies nur für hochspezialisierte Anbieter der IT-Branche gilt, täuscht sich. Der Einsatz von Encryption macht branchenübergreifend sowohl für Einzelunternehmer als auch multinationale Konzerne in vielerlei Hinsicht Sinn.

E-MAILS SICHER VERSCHLÜSSELN

Um Informationssicherheit durch Verschlüsselung zu erreichen, kann die Information selbst chiffriert werden. Dies wird als **inhaltliche Verschlüsselung** bezeichnet. Ein prominentes Beispiel hierfür ist **S/MIME** für E-Mails.

Die **Transportverschlüsselung** dagegen zielt auf den Kanal ab, der die Information überträgt. Dabei muss es sich nicht immer um die Übermittlung von E-Mails handeln, es kann auch um die Datenübertragung bei Websites gehen. Hier kommt beispielsweise **TLS/SSL** zum Einsatz.

So unterschiedlich wie die Arten von Daten, die im Internet weitergegeben werden, sind auch die Möglichkeiten von Encryption. Mittels **Code Signing** etwa fügen Software-Anbieter dem von ihnen zur Verfügung gestellten Programmcode eine digitale Unterschrift hinzu.
So kann sich der Empfänger beim Download darauf verlassen, dass die Anwendung tatsächlich vom Hersteller stammt und keine Schadsoftware von Dritten hinzugefügt wurde.

EINLEITUNG
KAPITEL 01
KAPITEL 02
KAPITEL 03
FAZIT

TRANSPORTVERSCHLÜSSELUNG MITTELS SSL

SSL steht für Secure Socket Layer. Layer bedeutet in dem Zusammenhang die Transportschicht zwischen zwei Rechnern, grob gesagt, den Kommunikationskanal. Während einer sicheren Verbindung kommunizieren die beteiligten Rechner ausschließlich über den von SSL bereitgestellten Mechanismus, der **Transportweg** wird verschlüsselt. Die Nachricht selbst bleibt im Klartext.

Im Zentrum der Funktionsweise von SSL steht das digitale Schlüsselpaar des Servers, also dessen öffentlicher und privater Schlüssel. Zudem werden digitale Zertifikate eingesetzt – die Schlüssel werden authentifiziert.

Eine verschlüsselte SSL-Verbindung geht immer vom Client aus, der eine Art digitale Begrüßung, den Handshake, startet. Hierzu kontaktiert er den Server. Dieser sendet sein SSL-Zertifikat an den Client zurück, der es auf seine Gültigkeit prüft. Zudem geht eine Anfrage an die Zertifizierungsstelle (Certification Authority, kurz CA), um auch die Signatur zu verifizieren.

Ist die Überprüfung erfolgreich beendet, erstellt der Client einen symmetrischen Schlüssel namens **Premaster Secret (PMS)**, codiert ihn mit dem öffentlichen Schlüssel des Servers und sendet ihn zurück. Der Server wiederum nutzt seinen privaten Schlüssel, um den PMS zu decodieren. Aus dem PMS generieren nun beide Seiten einen symmetrischen Schlüssel, der schließlich einen ebenfalls symmetrisch verschlüsselten Kommunikationskanal erstellt – die SSL-Verbindung ist fertig.

SSL nutzt also zunächst für den Handshake eine asymmetrische Verschlüsselung. Die spätere Datenübertragung dagegen läuft über eine symmetrische Verschlüsselung.

TLS/SSL-Zertifikate
Es existieren verschiedene Varianten von TLS/SSL-Zertifikaten, die vom Bedarf des Antragstellers abhängen. Sie unterscheiden sich z. B. in der Art der Validierung, ihrer Verschlüsselungsstärke oder darin, welche Browser sie unterstützen.

EINLEITUNG
KAPITEL 01
KAPITEL 02
KAPITEL 03
FAZIT

TRANSPORTVERSCHLÜSSE-LUNG MITTELS TLS

TLS (Transport Layer Security) ist kurz gesagt der Nachfolger von SSL. Das Protokoll wird seit 1996 entwickelt und trug zunächst den Namen SSL 3.1.
Seit 1999 lautet die offizielle Bezeichnung TLS, die aktuelle Version existiert seit 2018 und hat die Nummer 1.3.

Die prinzipielle Funktionsweise mit Handshake ist bei TLS und SSL identisch. Mit dem neuen TLS Protokoll wird jedoch die Sicherheit gegenüber Angriffen erhöht. Zudem unterstützt es noch mehr Algorithmen zur Verschlüsselung zwischen Server und Client. Aus diesen Gründen sollte heute TLS bevorzugt zum Einsatz kommen. Als Abkürzung ist SSL allerdings wesentlich bekannter. Daher wird nach wie vor meist von SSL gesprochen, wenngleich TLS gemeint ist.

Wer auf Nummer sicher gehen will, nutzt die Bezeichnung **TLS/SSL**.

BSI Empfehlung

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat im Zuge von COVID-19 und der daraus resultierenden Zunahme von Homeoffice den „Mindest-standard zur Verwendung von Transport Layer Security (TLS)“ aktualisiert. Für eine sichere Transportverschlüsselung sollten ausschließlich TLS 1.3 oder aber TLS 1.2 mit einem speziellen Verfahren zum Schlüsselaustausch (Diffie-Hellman-Protokoll) genutzt werden. Beide, TLS 1.2 und TLS 1.3, sind im Regelfall standardmäßig vorhanden.

EINLEITUNG
KAPITEL 01
KAPITEL 02
KAPITEL 03
FAZIT

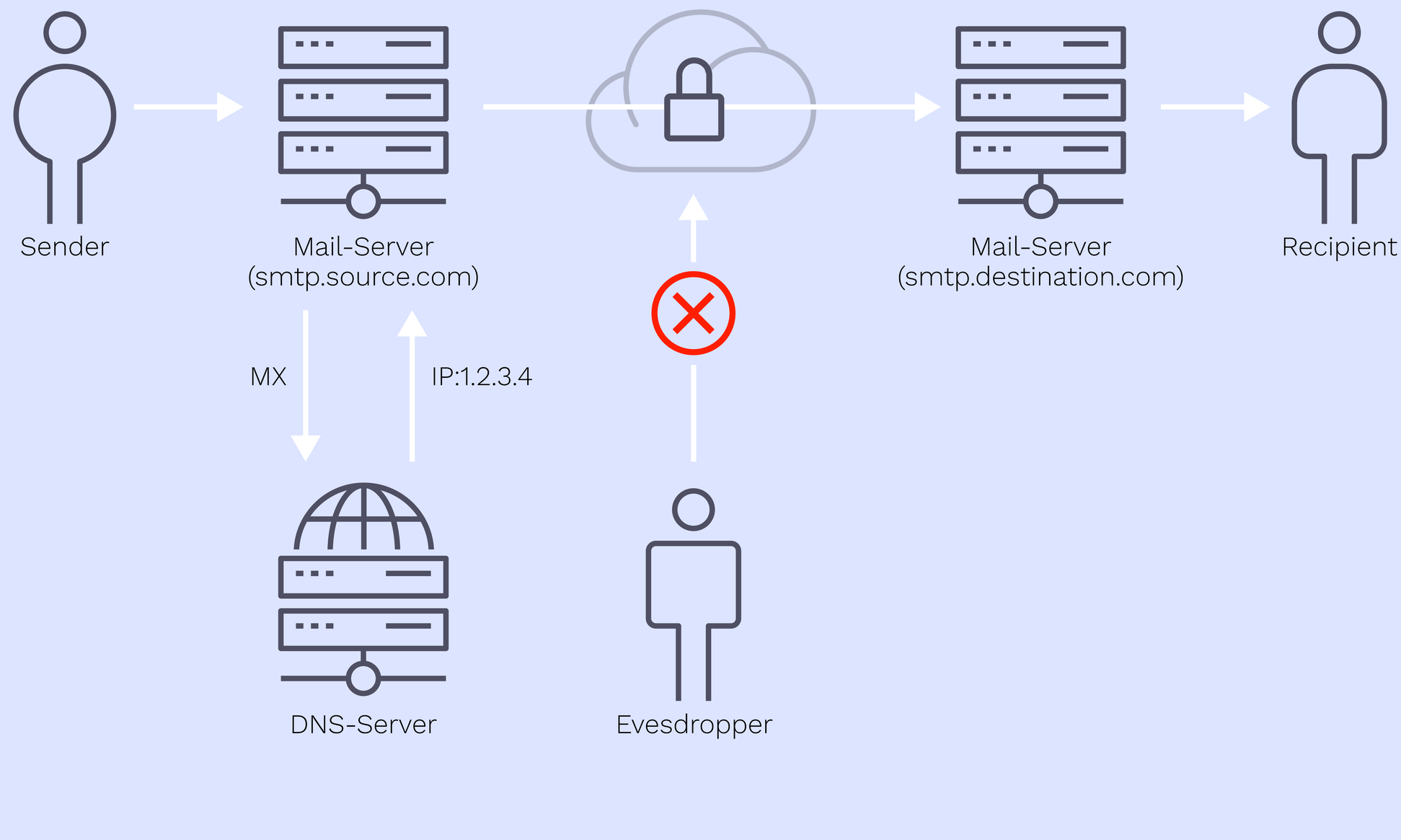
REICHT TRANSPORTVERSCHLÜSSELUNG FÜR EINEN SICHEREN UND DSGVO-KONFORMEN VERSAND AUS?

Wie erwähnt verschlüsseln **SSL** und **TLS** den Transportkanal, über den eine Nachricht übermittelt wird – nicht jedoch die Nachricht selbst. Am Anfang sowie am Ende des Übertragungswegs liegt die Nachricht auf den jeweiligen Servern unverschlüsselt vor.

Von dort bis zum Endgerät können Dritte die Information theoretisch abfangen oder manipulieren.

Vom Bayerischen Landesamt für Datenschutzaufsicht (BayLDA) kommt daher der Hinweis, dass die Verschlüsselung von E-Mails via TLS alleine nicht ausreicht. Transportverschlüsselung sollte aber ein zentraler Baustein der Sicherheitsmaßnahmen sein.

Um eine **End-to-End-Verschlüsselung** zu erreichen, die modernsten Ansprüchen genügt, sollten sich Unternehmen zusätzlich um eine Inhaltsverschlüsselung für ihre digitale Kommunikation kümmern. Dabei wird die Nachricht selbst direkt vom Absender codiert und erst auf dem Gerät des Empfängers wieder entschlüsselt. Damit erreichen alle Beteiligten die höchstmögliche Sicherheitsstufe, um Informationen digital auszutauschen.



EINLEITUNG
KAPITEL 01
KAPITEL 02
KAPITEL 03
FAZIT

E-MAIL-VERSCHLÜSSELUNG MIT S/MIME

S/MIME (Secure/Multipurpose Internet Mail Extensions) existiert seit 1995. Mit S/MIME lassen sich verschiedenste Daten verschlüsseln, E-Mails dürften jedoch der bekannteste Anwendungsfall sein.
S/MIME basiert – wie auch **PGP** (Pretty Good Privacy) – auf hybrider Verschlüsselung, also einer Kombination aus symmetrischer und asymmetrischer Encryption. Obwohl das Funktionsprinzip bei beiden vergleichbar ist, sind S/MIME und PGP nicht kompatibel. Man ist daher letztlich gezwungen, entweder alle Kommunikationspartner vom verwendeten Standard zu überzeugen oder zweigleisig zu fahren.

S/MIME bietet im Gegensatz zu PGP zusätzlich zur Verschlüsselung noch eine Signierfunktion. Die Nachricht bleibt dabei für alle sichtbar, es wird allerdings eine kryptographische Signatur hinzugefügt, die Empfänger verifizieren können. Ist die Signatur “in Ordnung”, wurde der Inhalt der E-Mail nicht manipuliert. Zudem spricht für S/MIME, dass das Verfahren mit vielen Mail-Clients kompatibel ist.

Als sogenannte **Client-Zertifikate** werden S/MIME-Zertifikate in personalisierter Form ausgestellt und pro Rechner installiert. Ein S/MIME-Zertifikat authentifiziert die jeweiligen User, die während des SSL-Handshakes durch den Austausch des Client-Zertifikats auf einen Server zugreifen.

Das bei S/MIME angewendete **Public-Key-Verfahren** (asymmetrische Verschlüsselung) nutzt ein Schlüsselpaar einen **Public Key** und einen **Private Key**. Jeder Schlüssel (Zertifikat) ist weltweit einmalig.

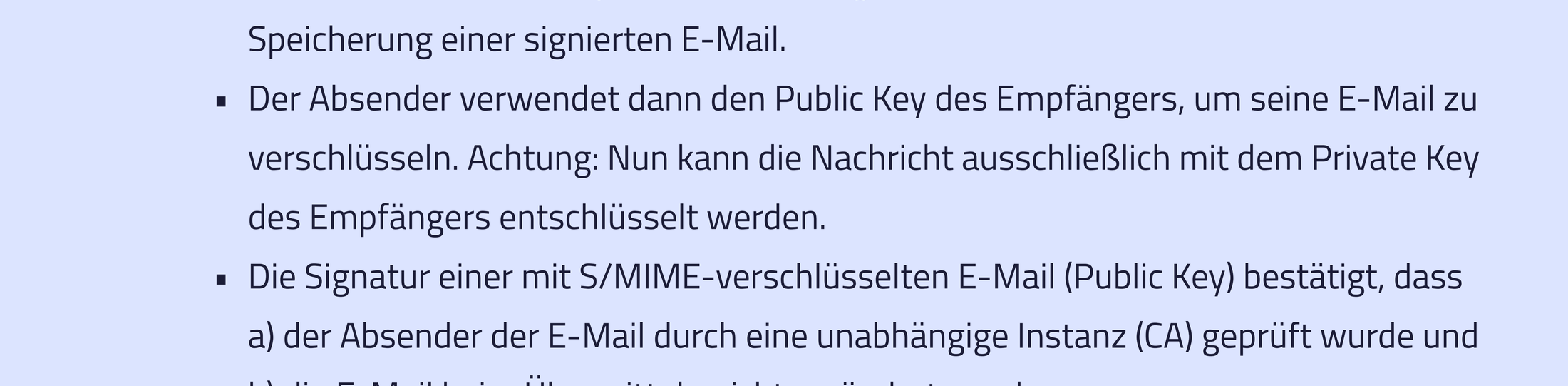
Wichtig dabei ist: der Private Key lässt sich nicht aus dem Public Key ableiten. Der Public Key dient der E-Mail-Codierung und wird dem Adressaten per E-Mail zum Tausch angeboten. So kann der Verschlüsselungsprozess funktionieren.

Der Austausch der öffentlichen Schlüssel per E-Mail zwischen Sender und Empfänger ist also die zentrale Voraussetzung für die Verschlüsselung.

EINLEITUNG
KAPITEL 01
KAPITEL 02
KAPITEL 03
FAZIT

SO FUNKTIONIERT DAS S/MIME-VERFAHREN IM DETAIL:

- Beide, Sender und Empfänger, verwenden ein E-Mail-Zertifikat und müssen zunächst ihre Public Keys tauschen. Das geschieht durch den Versand und die Speicherung einer signierten E-Mail.
- Der Absender verwendet dann den Public Key des Empfängers, um seine E-Mail zu verschlüsseln. Achtung: Nun kann die Nachricht ausschließlich mit dem Private Key des Empfängers entschlüsselt werden.
- Die Signatur einer mit S/MIME-verschlüsselten E-Mail (Public Key) bestätigt, dass a) der Absender der E-Mail durch eine unabhängige Instanz (CA) geprüft wurde und b) die E-Mail beim Übermitteln nicht verändert wurde.



S/MIME baut auf **Zertifizierungsstellen** (CAs wie zum Beispiel DigiCert). CAs stellen üblicherweise Zertifikate in drei bis vier unterschiedlichen Klassen aus.

EINLEITUNG
KAPITEL 01
KAPITEL 02
KAPITEL 03
FAZIT

KLASSE	BESCHREIBUNG
Klasse 1: Domain-validiert	Die CA prüft per E-Mail, ob die hinterlegte Domain und die E-Mail-Adresse existiert und nimmt auch nur diese Information in das Zertifikat mit auf. Diese erfüllen die Standards, eignen sich allerdings nur bedingt für den sehr sicheren und datenschutz-konformen Einsatz im geschäftlichen Kontext.
Klasse 2: Identitäts-validiert	Auch hier erfolgt eine Prüfung der E-Mail-Adresse. Darüber hinaus verifiziert sich der Antragsteller über eine Ausweiskopie, ein Unternehmen über den Handelsregisterauszug. Der Name der Person beziehungsweise der Firma ist mit der entsprechenden E-Mail-Adresse Bestandteil des Zertifikats.
Klasse 3: Organisations-validiert	Zusätzlich zu den Daten der Klasse 2 wird geprüft, ob eine Person tatsächlich zu einer bestimmten Organisation gehört. Hierzu erfolgt ein Anruf bei der Personalabteilung mit einer Nummer aus dem Telefonbuch. Darüber hinaus fordert die Zertifizierungsstelle einen Nachweis über den Handelsregistereintrag an.

EINLEITUNG
KAPITEL 01
KAPITEL 02
KAPITEL 03
FAZIT

Die unterschiedlichen Klassen bilden gleichzeitig unterschiedliche Vertrauensstufen ab. Bei einem Zertifikat der Klasse 3 etwa wird ein höherer Aufwand zur Verifizierung des Teilnehmers betrieben, bei Klasse 1 kann man sich lediglich sicher sein, dass die E-Mail-Adresse existiert.

Eine sichere Verschlüsselung gelingt mit Zertifikaten aller Klassen, da die verwendeten Algorithmen jeweils identisch sind.

Auch die DSGVO-Konformität ist, nach aktuellem Stand, weitgehend gesichert.

REICHT EINE INHALTS-VERSCHLÜSSELUNG AUS?

Die Verschlüsselung des Inhalts macht zwar den Nachrichtentext und etwaige Anhänge für Dritte unlesbar, wichtige Metadaten sind jedoch nicht geschützt. Die E-Mail-Adresse von Absender und Empfänger sowie der Betreff der Nachricht sind weiterhin offen zugänglich.

Eine echte End-to-End-Verschlüsselung der kompletten Nachricht lässt sich nur erreichen, wenn Inhaltsverschlüsselung und Transportverschlüsselung kombiniert werden. Der Sender verschlüsselt und signiert zunächst via S/MIME den Inhalt der E-Mail. Um dann einen sicheren Kommunikationskanal zu erstellen und die Metadaten zu schützen, kommt die Transportverschlüsselung mit TLS zum Einsatz. Beim Empfänger angekommen, wird die Nachricht entschlüsselt und die digitale Signatur geprüft. So wird sichergestellt, dass die E-Mail authentisch, unverändert und vertraulich ist.

EINLEITUNG
KAPITEL 01
KAPITEL 02
KAPITEL 03
FAZIT

Best Practice: E-Mail-Verschlüsselung für Unternehmen.

Um gesetzlichen Anforderungen gerecht zu werden und sensible Daten hinreichend zu schützen, führt an Verschlüsselung kein Weg vorbei. Der Schutz von Vertraulichkeit und Integrität personenbezogener Daten bei der Übermittlung von E-Mails setzt voraus, dass Sender und Empfänger zusammenwirken und Standards einhalten.

> **Artikel 32 DSGVO** nennt mögliche Sicherungsmaßnahmen, die unter Berücksichtigung
>
> - des Stands der Technik,
> - der Implementierungskosten,
> - der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie
> - der unterschiedlichen Eintrittswahrscheinlichkeit und
> - Schwere des Risikos für die Rechte und Freiheiten
>
> natürlicher Personen zu treffen sind.

Die Verantwortung für den einzelnen Übermittlungsvorgang liegt beim Sender. Wer jedoch gezielt personenbezogene Daten per E-Mail entgegennimmt, ist ebenso verpflichtet, die nötigen Voraussetzungen für den sicheren Empfang von E-Mail-Nachrichten über einen verschlüsselten Kanal zu schaffen – und diese auch sicher zu verwahren.

EINLEITUNG
KAPITEL 01
KAPITEL 02
KAPITEL 03
FAZIT

Diese Fragen sind zu klären:

- Sind alle E-Mails zu verschlüsseln?
- Welche technischen Voraussetzungen müssen geschaffen werden?
- Welcher Partner hilft bei der Umsetzung?

BESTANDSAUFNAHME: WELCHE DATEN VERSENDET MEIN UNTERNEHMEN?

Die DSGVO empfiehlt, E-Mails zu verschlüsseln. Eine direkte Pflicht besteht bislang nicht – werden die Vorgaben jedoch nicht beachtet und es kommt zu einer Datenpanne, müssen die betroffenen Personen binnen 72 Stunden darüber informiert werden und können gegebenenfalls rechtliche Ansprüche geltend machen.

Gelangen Daten in die falschen Hände, droht eine große wirtschaftliche Gefahr, vom Vertrauensverlust in das Unternehmen ganz zu schweigen. Werden in einer Nachricht personenbezogene Daten verarbeitet, sollten diese also unbedingt verschlüsselt werden.

Zu **personenbezogene Daten** zählen beispielsweise:

- Postadresse
- Telefonnummer
- Kontoverbindung
- Zahlungsdaten
- Kundennummer
- u. U. IP-Adresse

Bei **sensiblen Daten** handelt es sich um besonders schützenswerte personenbezogene Informationen:

- kulturelle Herkunft
- biometrische Daten
- politische, religiöse und philosophische Überzeugungen
- Sexualität und Gesundheit
- Zugehörigkeit zu einer Gewerkschaft

EINLEITUNG
KAPITEL 01
KAPITEL 02
KAPITEL 03
FAZIT

DIESE MASSNAHMEN SOLLTEN UNTERNEHMEN TREFFEN

1 Starten Sie mit einem **Audit** und einer **Schutzbedarfsanalyse**, die zentrale W-Fragen klären: Wer schickt, wie häufig, welche sensiblen Daten an welchen Empfänger? Und welchen Standards entspricht die momentan zugrundeliegende IT-Infrastruktur? Mindert diese das Datenleckrisiko? Und entspricht sie auch den rechtlichen Anforderungen?

2 **Verschlüsselung macht nur Sinn, wenn alle im Team ihre Bedeutung erkennen und sie korrekt umsetzen. Weiterbildungsmaßnahmen und firmeninterne Leitfäden zur E-Mail-Nutzung und deren Codierung helfen dem Team bei der praktischen Anwendung der Sicherheitsmaßnahmen.**

3 Datenschützer sind sich einig:
E-Mails mit **personenbezogenen**, **sensiblen** oder **geschäftskritischen Daten** sollten in jedem Fall verschlüsselt werden.

4 **Übertragen Abteilungen häufig sensible Daten (intern oder extern), können sie diese Daten zusätzlich mit Passwörtern schützen und die Passwörter auf einem separaten Kommunikationskanal weitergeben.**

EINLEITUNG
KAPITEL 01
KAPITEL 02
KAPITEL 03
FAZIT

5 Sowohl Transportverschlüsselung als auch Inhaltsverschlüsselung alleine lassen mögliche Einfallstore für Datenspionage offen. Für größtmögliche Sicherheit sollten beide kombiniert und/oder **S/MIME** eingesetzt werden.

6 **Lässt sich intern die End-to-End-Verschlüsselung nicht realisieren, sollten Inhalt und Transportweg von Nachrichten zumindest ab dem Zeitpunkt codiert werden, an dem sie das Unternehmensnetzwerk verlassen. Nach Möglichkeit sollte auch die interne Kommunikation verschlüsselt werden.**



7 Je nach **Set-up der Daten- und E-Mail-Infrastruktur** ist zu prüfen, ob S/MIME für die Inhaltsverschlüsselung notwendig und geeignet ist. Werden alle Clients unterstützt? Reicht das Web of Trust (PGP) als Vertrauensbasis aus oder sollten allgemein anerkannte Zertifikate in möglichst hoher Vertrauensstufe genutzt werden? Für die meisten Unternehmen stellt sich nach Abwägung dieser Fragen S/MIME als die bessere Alternative heraus, um höchstmögliche Sicherheit zu bieten und Risiken zu vermindern.

8 **Kompetente Partner unterstützen bei der Auswahl der passenden Zertifikate für die Verschlüsselung. Im besten Fall liefern sie Lösungen sowohl für Inhalts- als auch Transportverschlüsselung und orientieren sich dabei am zur Verfügung stehenden Budget.**



EINLEITUNG
KAPITEL 01
KAPITEL 02
KAPITEL 03
FAZIT

WER HILFT BEI DER UMSETZUNG?

Sie wollen eine Transportverschlüsselung oder Inhaltsverschlüsselung einrichten? Dann agieren Sie DSGVO-konform und sind rechtlich auf der sicheren Seite. Das Team von InterNetX berät Sie bei Ihren Fragen zu TLS/SSL und S/MIME.

Mit Produkten namhafter Anbieter wie DigiCert finden wir für Unternehmen jeder Größenordnung und für jedes Budget die passende Lösung. Über die Domain- und TLS/SSL-Plattform AutoDNS können Sie Ihre Zertifikate unkompliziert verwalten.

S/MIME-Zertifikate in unterschiedlichen Vertrauensstufen sichern sensible und personenbezogene Daten, die innerhalb des Unternehmens und an Kunden und Partner verschickt werden.

EINLEITUNG
KAPITEL 01
KAPITEL 02
KAPITEL 03
FAZIT

Encryption: Chance und Lösung.

Phishing, Datenverlust und -missbrauch sowie rechtliche Rahmenbedingungen machen E-Mail-Verschlüsselung für Unternehmen zu einem Muss.

Hybride Encryptionverfahren und End-to-End-Lösungen bieten größtmögliche Sicherheit. Mittlerweile existieren viele benutzerfreundliche Lösungen, die Firmen kosteneffizient implementieren können, um das Datendiebstahlrisiko in der E-Mail-Kommunikation zu minimieren.

Internet Service Provider wie InterNetX unterstützen Sie dazu mit kompetenter Beratung und den passenden Produkten für die DSGVO-konforme Verschlüsselung Ihrer E-Mails.

Weitere Ressourcen.

- Bundesdatenschutzgesetz (BDSG): § 22 Verarbeitung besonderer Kategorien personenbezogener Datensonenbezogener Daten
- Bundesdatenschutzgesetz (BDSG): § 64 Anforderungen an die Sicherheit der Datenverarbeitung
- How does the GDPR affect email?

EINLEITUNG
KAPITEL 01
KAPITEL 02
KAPITEL 03
FAZIT

Quellenangaben.

- dsgvo-gesetz.de
- Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG)
- Statista Research Department: Prognose zur Anzahl der täglich versendeten und empfangenen E-Mails weltweit bis 2024
- Studie Deutschland Digital 2020 im Auftrag von WEB.DE und GMX (Repräsentative Studie der Convios Consulting GmbH)
- IHK Mittelfranken: FAQ Fragen an das BayLDA zur Ausgestaltung der DSGVO in der Praxis

Bildnachweis.

- Coverbild: Joanna Kosinska auf Unsplash

About.

Mit rund 4 Mio. verwalteten Domains gehört InterNetX zu den führenden Anbietern von White-Label-Produkten im Bereich von Hosting und Domains. Als ausgezeichneter Experte in Sachen Website & E-Mail Encryption und als DigiCert Platinum Elite Certified Partner bietet das Unternehmen auf seiner all-in-one Domain und SSL Management Plattform AutoDNS eine große Bandbreite an hochwertigen Zertifikaten weltweiter Marktführer an.

InterNetX GmbH
Johanna-Dachs-Str. 55
93055 Regensburg
Germany
Tel. +49 941 59559-0
Fax +49 941 59559-55
E-Mail: info@internetx.com
www.internetx.com

Follow us:

Abonnieren Sie unseren Newsletter:
www.internetx.com/internetxpress

Our Premium Platform Partner

digicert®

InterNetX