InterNetX

FÜR MEHR SICHERHEIT IM E-MAIL-VERKEHR

E-MAIL SECURITY

WHITEPAPER

WWW.INTERNETX.COM

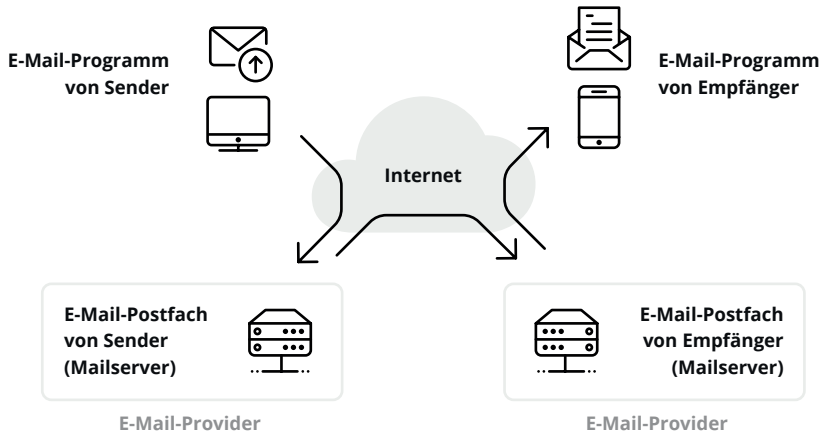
INHALTSVERZEICHNIS

EINLEITUNG

Spätestens mit Inkrafttreten der Datenschutz-Grundverordnung (DSGVO) am 25. Mai 2018 hat das Thema Datensicherheit auch in deutschen Unternehmen Einzug gehalten – oder etwa nicht? An der Zeit wäre es jedenfalls: Laut Bitkom-Umfrage ist fast die Hälfte aller Befragten (49 %) 2017 Cyberkriminalität zum Opfer gefallen, 54 % davon erlitten sogar finanzielle Schäden. Insgesamt belief sich der finanzielle Schaden in Deutschland – verursacht durch Computerbetrug, Datenveränderung und Co. – in besagtem Jahr auf sage und schreibe 71,8 Mio. Euro.

Welche Gefahr von Cyberkriminalität speziell in der heutigen Geschäftswelt ausgeht, verdeutlicht der bis dato größte Unternehmens-Hack in der Geschichte des Internets. Ziel des Angriffs: Der US-amerikanische Filmkonzern Sony Pictures Entertainment. Im November 2014 verschafften sich Unbekannte Zugriff zu den Servern des Entertainment-Giganten, fertigten rund 100-Terabyte-große Kopien sensibler Daten an und veröffentlichten diese anschließend online, darunter auch streng vertraulicher E-Mail-Verkehr. Die traurige Realität: Im Grunde hätte Sony Pictures Entertainment seine Daten mit nur geringem Aufwand schützen können – nämlich mittels Verschlüsselung.

Vielen Personen – ob im privaten oder geschäftlichen Kontext – ist gar nicht bewusst, wie leichtsinnig sie E-Mails versenden. Stellen Sie sich vor, Sie verschicken einen Brief klassisch per Post, verzichten aber auf den Briefumschlag: Jeder, der den Brief in die Hände bekommt, kann prinzipiell problemlos mitlesen. Nicht anders ist das bei unverschlüsselter E-Mail-Kommunikation.



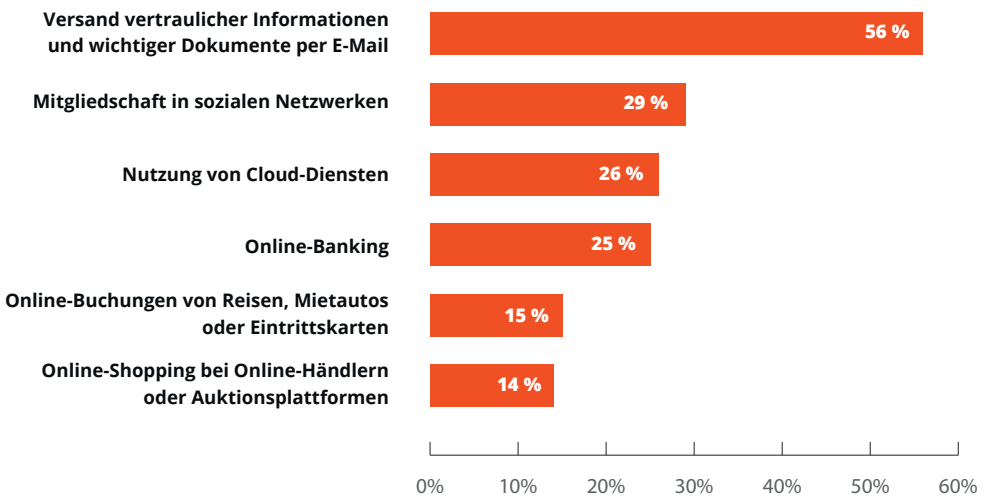
Funktionsweise der E-Mail-Kommunikation

Doch gerade die Verschlüsselung von E-Mails wird in der Praxis heute noch relativ stiefmütterlich behandelt. Zwar gaben bei einer Umfrage im Auftrag von WEB.DE und GMX zur Wichtigkeit von E-Mail-Verschlüsselung knapp zwei Drittel der Teilnehmer an, ihnen sei die Thematik wichtig oder zumindest eher wichtig, tatsächlich genutzt wurde die E-Mail-Verschlüsselung 2018 jedoch gerade einmal von 13,5 %. Bedenkt man, dass allein in Deutschland im Jahre 2017 ungefähr 771 Mrd. E-Mails versandt wurden, ist hier also definitiv noch Potenzial nach oben. Denn speziell im geschäftlichen Bereich sind von Tag zu Tag unzählige E-Mails mit Geschäftsgeheimnissen und sensiblen, oftmals personenbezogenen Inhalten im Umlauf.

Mithilfe dieses Whitepapers möchten wir Ihnen einen umfassenden Einblick in die Welt der E-Mail-Sicherheit gewähren. Bevor der Fokus dabei auf den gängigen Sicherheitsstandard S/MIME (Secure / Multipurpose Internet Mail Extensions) zur E-Mail-Verschlüsselung und -Signatur gelegt wird, soll einführend vor allem die heutige Wichtigkeit und allgemeine Funktionsweise von E-Mail-Verschlüsselung erläutert werden.

GEFAHRENZONE
E-MAIL

Die Angst vor Cyberkriminalität ist in der deutschen Bevölkerung angekommen: Einer 2018 durchgeführten Umfrage zufolge verzichten 56 % der Befragten aus Sicherheitsbedenken auf den Versand vertraulicher Informationen und wichtiger Dokumente per E-Mail. Die E-Mail-Kommunikation gilt damit in Deutschland als die am wenigsten vertrauenswürdige Online-Aktivität – noch vor Social Media, Cloud Services und Online Banking.

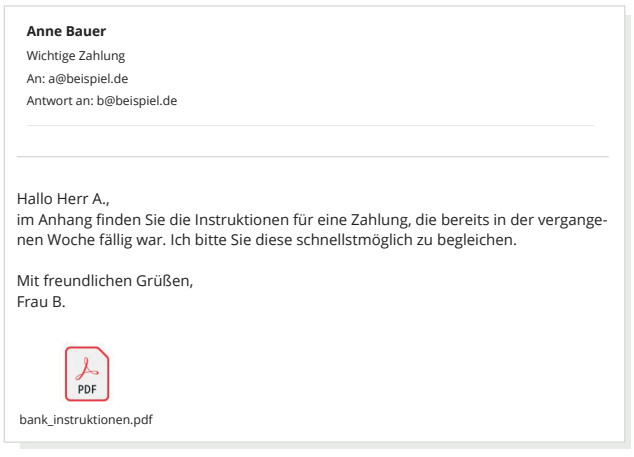


Quelle: Bitkom

Weitere Informationen: Deutschland; Bitkom Research; 2017; 1.017 Internetnutzer; ab 14 Jahre; nur die Internetnutzer, die auf Online-Aktivitäten verzichten

Eine weit verbreitete Gefahr im Zusammenhang mit E-Mails ist die Phishing-Variante Spoofing, bei dem ein oder mehrere Hacker eine E-Mail nach Vorbild eines seriösen Absenders, zum Beispiel einem Unternehmen, fälschen. Der Clou dabei: Die Empfänger sollen die E-Mail als Original wahrnehmen, vertrauenswürdig einstufen und infolgedessen bereit sein, ohne Bedenken personenbezogene Daten weiterzugeben bzw. infizierte E-Mail-Anhänge herunterzuladen. Richtet sich eine solche E-Mail-Fälschung an eine einzelne Person bzw. Organisation, ist von Spear Phishing die Rede. Bei dieser Phishing-Variante werden die Inhalte individuell an den jeweiligen Empfänger angepasst, sie erscheinen für ihn also grundsätzlich noch glaubwürdiger.

Auch sogenannte Man-in-the-Middle-Angriffe stehen heute längst an der Tagesordnung. Bei einer solchen Attacke wird die E-Mail-Kommunikation von einer außenstehenden Instanz abgefangen. Ziel dabei ist es, E-Mail-Inhalte einzusehen und im schlimmsten Fall sogar zu manipulieren.



E-Mail-Spoofing stellt eine große Gefahr dar

E-MAIL-SICHERHEIT
IN ZEITEN DER DSGVO

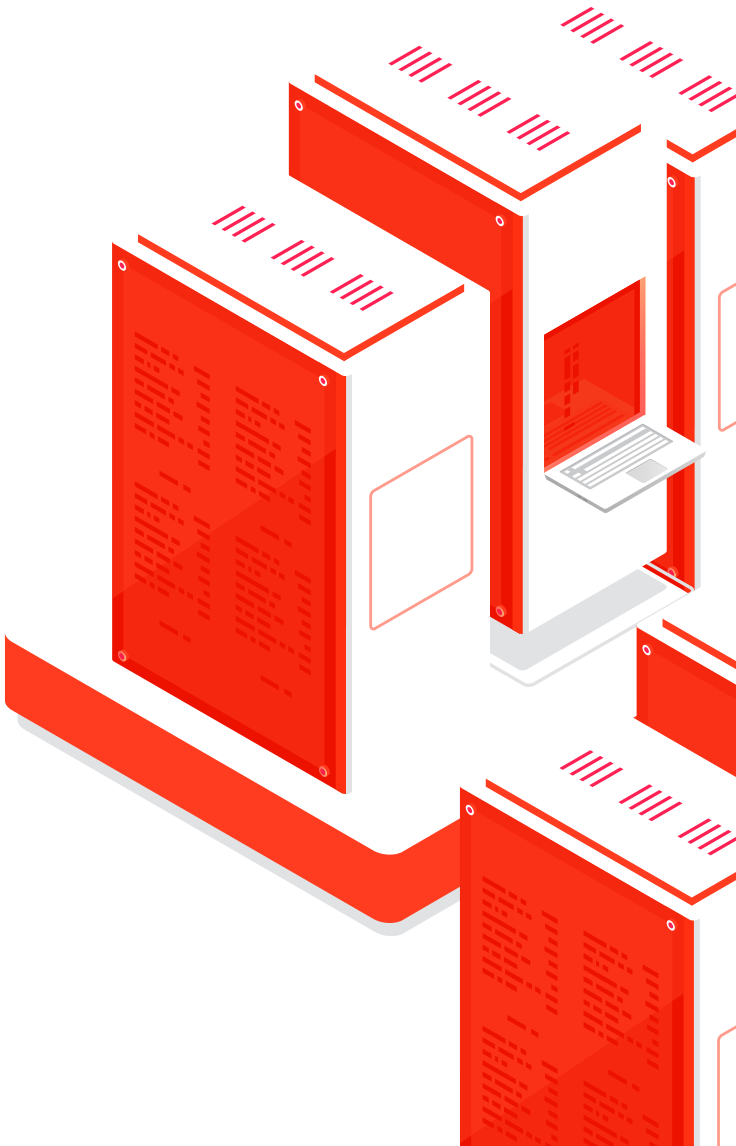
Gerade mit Blick auf die Datenschutz-Grundverordnung (DSGVO) hat das Thema E-Mail-Verschlüsselung – zumindest in der Theorie – massiv an Bedeutung gewonnen. Speziell Artikel 32 (Sicherheit der Verarbeitung) der DSGVO nimmt hierzu ausführlich Bezug:

“Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und 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 treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.”

Zu besagten Maßnahmen zählt die DSGVO unter anderem auch “die Pseudonymisierung und Verschlüsselung personenbezogener Daten”. Dementsprechend sind Unternehmen heute eigentlich sogar dazu verpflichtet, ihre E-Mails zu verschlüsseln, wenn auf diesem Wege personenbezogene Daten ausgetauscht werden. Die Praxis lässt jedoch ein anderes Bild erkennen: Im September 2018 war lediglich in einem knappen Viertel der deutschen Unternehmen (24 %) die Umsetzung der DSGVO bereits vollständig abgeschlossen, 30 % hatten sie zu diesem Zeitpunkt gerade einmal teilweise verwirklicht.

In der Unternehmenspraxis besteht heute leider noch oftmals der Irrglaube, dass ein SSL-Zertifikat auf dem eigenen Mail-Server bereits genügt, um für vollständigen Schutz in der E-Mail-Kommunikation zu sorgen. Theoretisch kann ein SSL-Zertifikat zwar dabei helfen, Man-in-the-Middle-Angriffe zu verhindern, jedoch besteht nur hinsichtlich der eigenen Mail-Server die Gewissheit, dass diese tatsächlich via SSL-Zertifikat geschützt wurden. Ob die sonstigen Mail-Server, die die E-Mail bei der Übertragung durchläuft, über ein SSL-Zertifikat verfügen und somit ausreichend Schutz bieten, bleibt fraglich.

Aus diesem Grund raten Experten dazu, nicht nur eine Mail-Server-Sicherung mittels SSL-Zertifikat durchzuführen, sondern auch die E-Mail selbst zu verschlüsseln.



KURZ ERKLÄRT:
E-MAIL-VERSCHLÜSSELUNG

Die Verschlüsselung von E-Mails erfolgt entweder auf symmetrische oder asymmetrische Weise. Während bei der symmetrischen Verschlüsselung derselbe Schlüssel zur Ver- und Entschlüsselung der Daten verwendet wird, kommen bei der asymmetrischen Verschlüsselung zwei unterschiedliche Schlüssel zum Einsatz, ein öffentlicher Schlüssel für die Verschlüsselung und ein privater Schlüssel für die Entschlüsselung. Im privaten Schlüssel liegt auch der grundlegende Vorteil der asymmetrischen Verschlüsselung: Auch wenn jemand den öffentlichen Schlüssel kennt, lässt sich der private Schlüssel nicht mit dessen Hilfe errechnen. Bei der symmetrischen Verschlüsselung hingegen ist es notwendig, den öffentlichen (und einzig verfügbaren) Schlüssel gegenüber Unbefugten geheimzuhalten.

SYMMETRISCHE VERSCHLÜSSELUNG

› Ein öffentlicher Schlüssel zum Ver- und Entschlüsseln

ASYMMETRISCHE VERSCHLÜSSELUNG

Zwei Schlüssel

› Ein öffentlicher Schlüssel zum Verschlüsseln

› Ein privater Schlüssel zum Entschlüsseln

Symmetrische vs. asymmetrische Verschlüsselung

Grundlage für die asymmetrische Verschlüsselung bildet die sogenannte Public Key Infrastructure (PKI). Durch das Ausstellen von Zertifikaten, die die Echtheit und Gültigkeit einer Identität zu einem bestimmten Zeitpunkt bestätigen, ermöglicht die PKI auch in unsicheren Netzwerken einen sicheren Datenaustausch.

In der Praxis hat sich besonders ein Verfahren zur Verschlüsselung von E-Mails durchgesetzt: S/MIME bzw. Secure/Multipurpose Internet Mail Extensions, welches sich der sogenannten hybriden Verschlüsselung bedient, einer Mischform aus symmetrischer und asymmetrischer Verschlüsselung.

DER STANDARD FÜR E-MAIL-SICHERHEIT: **S/MIME**

Der oftmals mit S/MIME abgekürzte Standard Secure/Multipurpose Internet Mail Extensions wurde 1999 eingeführt, um für mehr Sicherheit in der E-Mail-Kommunikation zu sorgen. Voraussetzung dafür: Beide Kommunikationspartner nutzen die S/MIME-Technologie. S/MIME basiert auf X.509-Zertifikaten und wird von der Internet Engineering Task Force (IETF) verfolgt. Durch folgende zwei Funktionen erhöht S/MIME die E-Mail-Sicherheit maßgeblich:

- **E-MAIL-VERSCHLÜSSELUNG**
- **E-MAIL-SIGNATUREN**

Bereits 1995 wurde der Grundstein für S/MIME im RFC 1847 gelegt: Damals wurden für den E-Mail-Standard MIME (Multipurpose Internet Mail Extensions) zwei Sicherheitserweiterungen definiert, einmal zur E-Mail-Signierung und einmal zur E-Mail-Verschlüsselung. Erstgenannte Erweiterung, das multipart/signed-Format, findet auch heutzutage bei S/MIME Anwendung. Zur E-Mail-Verschlüsselung wird hingegen das eigens für S/MIME entwickelte application/pkcs7-mime eingesetzt.

Bei Interesse an S/MIME-Zertifikaten gelten nicht nur offizielle Zertifizierungsstellen (CA), wie GlobalSign, als Anlaufpunkt, auch über Anbieter, zum Beispiel InterNetX als autorisierter GlobalSign-Partner, sind sie erhältlich. Nach erfolgreichem Antrag wird dem Benutzer ein öffentlicher und ein privater Schlüssel für das Ver- und Entschlüsseln sowie das Signieren von E-Mails übermittelt. Standardmäßig müssen S/MIME-Zertifikate nach einer gewissen Zeit (Laufzeit abhängig vom Anbieter) erneuert werden. Je nach Ausmaß der Überprüfung durch das CA werden die Zertifikate typischerweise einer von insgesamt drei Klassen zugeordnet und die überprüften Daten im Zertifikat ausgewiesen:

KLASSE 1

- **Echtheit der E-Mail-Adresse** (max.mustermann@beispiel.de)

KLASSE 2

- **Echtheit der E-Mail-Adresse** (max.mustermann@beispiel.de)
- **Name** (Max Mustermann)
- **Verifizierung über Ausweiskopie**

KLASSE 3

- **Echtheit der E-Mail-Adresse** (max.mustermann@beispiel.de)
- **Name und Unternehmen** (Max Mustermann; Beispielfirma GmbH)
- **Verifizierung über Personalausweis bzw. Handelsregisterauszug**

Die drei S/MIME-Zertifizierungsklassen

Wie funktioniert die Verschlüsselung und Signatur von E-Mails über S/MIME?

Abhängig davon, ob eine E-Mail verschlüsselt oder signiert wird, werden der öffentliche und private Schlüssel unterschiedlich eingesetzt.

E-MAIL-SICHERHEIT MIT S/MIME: VERSCHLÜSSELUNG

Nehmen wir an, Herr A. plant, Frau B. eine geschäftliche E-Mail zuzusenden. Da die Nachricht sensible Unternehmensdaten beinhaltet, möchte Herr A. die E-Mail über S/MIME verschlüsseln. Einzige Voraussetzung: Herr A. und Frau B. verfügen beide über ein S/MIME-Zertifikat und haben vorab mindestens einmal signierte E-Mails miteinander ausgetauscht. Neben der Geheimhaltung der Daten bezweckt Herr A. mit der Verschlüsselung ebenfalls, die Integrität der Nachricht zu wahren, das heißt dass die E-Mail auch wirklich unverändert bei Frau B. ankommt.

Zunächst erfolgt die symmetrische Verschlüsselung der im E-Mail-Klartext befindlichen Daten mittels öffentlichem Schlüssel. Im nächsten Schritt wird der öffentliche Schlüssel selbst verschlüsselt – und zwar mithilfe des S/MIME-Zertifikats von Frau B., das der E-Mail anschließend zum Zwecke der Nachvollziehbarkeit angehängt wird. Dank dieser Vorgehensweise weiß die Verschlüsselungssoftware von Frau B. genau, welcher private Schlüssel zur Entschlüsselung benötigt wird. Hat die E-Mail ihr Ziel – in unserem Beispiel Frau B. – erreicht, entschlüsselt der private Schlüssel den öffentlichen Schlüssel, um Frau B. die E-Mail in ihrer Ursprungsform anzuzeigen.

Falls Sie sich fragen, wer sich für das aufwendige Management von Zertifikaten und öffentlichen Schlüsseln verantwortlich zeigt: Diese Aufgabe übernehmen automatisierte Zertifikatsserver der jeweiligen CA.

Nachricht mit Session Key symmetrisch verschlüsselt

Versand: Session Key mit Empfängerzertifikat verschlüsselt

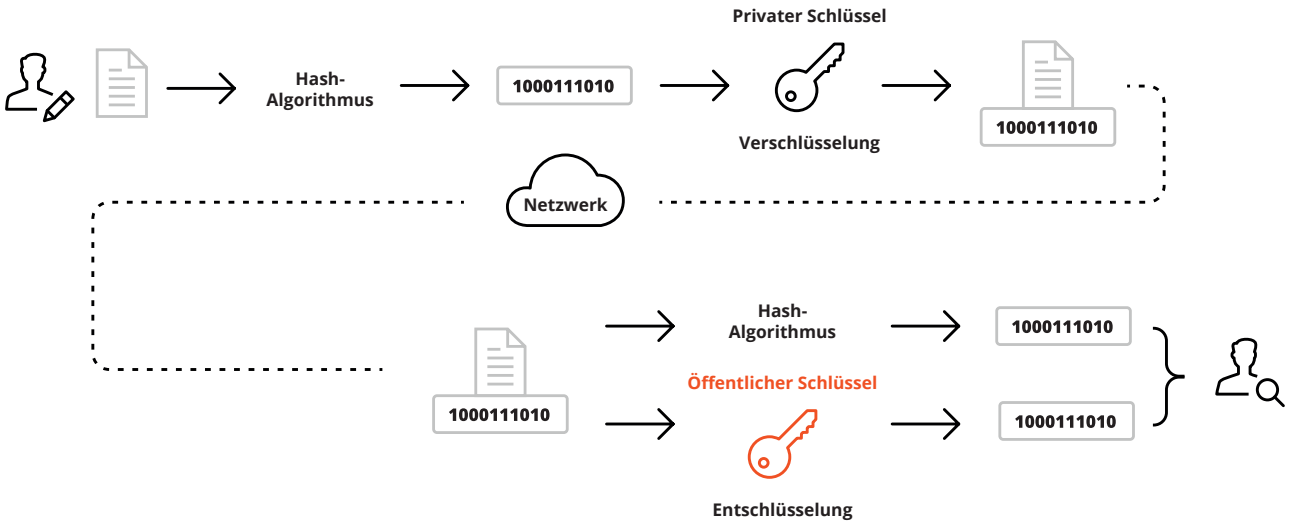
Privater Empfängerschlüssel entschlüsselt Session Key, dieser öffnet die Nachricht

So funktioniert die E-Mail-Verschlüsselung via S/MIME

E-MAIL-SICHERHEIT MIT S/MIME: DIGITALE SIGNATUR

Zusätzlich zur Verschlüsselung möchte Herr A. seine E-Mail gleichzeitig digital signieren – nur so kann Frau B. Herr A. als tatsächlichen Absender der Nachricht authentifizieren. Ein weiterer Vorteil für Frau B.: Herr A. kann nachträglich nicht leugnen, dass er die betreffende E-Mail versandt hat. Darüber hinaus fördert auch eine E-Mail-Signatur die Nachrichtenintegrität.

Im Gegensatz zur E-Mail-Verschlüsselung ist bei der E-Mail-Signatur der private Schlüssel des Absenders vonnöten: Bevor die Nachricht an Frau B. versendet wird, signiert Herr A. diese mithilfe seines privaten Schlüssels. Bei Erhalt der E-Mail sorgt auf Seiten von Frau B. der öffentliche Schlüssel für eine Verifizierung des Absenders.



So funktioniert die E-Mail-Signierung via S/MIME

Darum ist S/MIME die ideale Lösung für Unternehmen

Die Einführung von E-Mail-Verschlüsselung und digitaler Signaturen im Unternehmen ist mit einem hohen Zeit- und Arbeitsaufwand verbunden, oder? Nicht zwingend: S/MIME bietet einige Vorteile, die das Gegenteil beweisen.

VORTEIL 1: S/MIME IST MIT DEN GÄNGIGEN E-MAIL-CLIENTS KOMPATIBEL

Outlook, Thunderbird, Apple Mail, IBM Notes – die Liste der E-Mail-Clients, die S/MIME unterstützen, ist lang. Besonders softwarebasierte E-Mail-Clients sind längst mit S/MIME kompatibel, aber auch die Zahl webbasierter E-Mail-Clients nimmt seit geraumer Zeit zu: So können heute beispielsweise bereits via Outlook 365 oder Gmail verschlüsselte und signierte E-Mails verschickt werden.

VORTEIL 2: S/MIME ÜBERZEUGT DURCH BENUTZERFREUNDLICHKEIT

Wer kennt es nicht: Werden am Arbeitsplatz neue Programme, Tools oder Erweiterungen installiert, kann es unter Umständen eine gewisse Zeit dauern bis man sich an deren Nutzung gewöhnt hat. Bei S/MIME tritt dieses Problem nicht auf: Fast alle E-Mail-Clients ermöglichen es dem Benutzer beim Verfassen einer E-Mail, selbige per einfachem Klick zu verschlüsseln und/oder zu signieren. Die Empfänger erkennen durch eindeutige Symbole sofort, dass es sich um eine verschlüsselte und/oder signierte E-Mail handelt.

VORTEIL 3: S/MIME FUNKTIONIERT AUCH BEI MOBILGERÄTEN

Die Installation von S/MIME-Zertifikaten ist nicht nur auf dem Desktop möglich, auch auf mobilen Endgeräten lassen sich E-Mail-Verschlüsselung und -Signatur mit S/MIME problemlos umsetzen. Um auf mehreren Geräte dasselbe Zertifikat verwenden zu können, muss lediglich die genutzte E-Mail-Adresse übereinstimmen und der private Schlüssel bei Erstinstallation als exportierbar gesetzt werden – einer sicheren, geräteübergreifenden E-Mail-Kommunikation steht also nichts im Weg!

VORTEIL 4: S/MIME FÜR VERSCHIEDENE UNTERNEHMENSGRÖSSEN

Ob Sie als Einzelperson auf die S/MIME-Technologie zurückgreifen, einer kleinen Gruppe im Unternehmen E-Mail-Sicherheit gewährleisten oder im gesamten Unternehmen S/MIME nutzen möchten, erstklassige Anbieter, wie InterNetX, bieten Ihnen die passende Lösung für Ihre Anforderungen.

FAZIT

Kurz zusammengefasst: E-Mail-Sicherheit ist in der heutigen, von Cyberkriminalität geprägten Zeit wichtiger denn je. Akute Bedrohungen, wie Phishing-Versuche oder Man-in-the-Middle-Angriffe, machen es zukünftig unverzichtbar, E-Mails zu verschlüsseln und zu signieren. Mit S/MIME steht Ihnen eine anwenderorientierte und kostengünstige Lösung zur Verfügung, um Ihre E-Mails (und Daten) auf professionelle Weise vor unbefugten Zugriffen zu schützen.

InterNetX bietet Ihnen als GlobalSign Authorized Partner S/MIME-Zertifikate der offiziellen Zertifizierungsstelle an.

internetx.com/ssl-zertifikate/smime

InterNetX GmbH
Johanna-Dachs-Str. 55
93055 Regensburg
Deutschland

Tel. +49 941 59559-0
Fax +49 941 59559-55
E-Mail: info@internetx.com

InterNetX

WWW.INTERNETX.COM