Kundeninformation "email-Verschlüsselung und die DSGVO"

id newmedia KnowHow - für *Sie ...*

40 Jahre Erfahrung, 40 Jahre Dienst am Kunden

- ganzheitliche, sichere IT-Lösungen auch für kleinste Unternehmen
- ganzheitliche, sichere IT-Lösungen für Behörden
- DSGVO / BDSG-neu Umsetzung
- Analyse kritischer IT-Sicherheitsstrukturen
- Digitales Klassenzimmer in Schulen
- Digitales Büro
- Computer Forensik

id newmedia Einsteinstrasse 24 82152 Planegg-Martinsried 0160-48 28 918
id newmedia Büro Germering 089-899 799 39 info@id-newmedia.de www.id-newmedia.de USt.-Id Nr. DE128145303

Bild : animationfactory

Sind Sie laut Datenschutzgrundverordnung dazu verpflichtet, geschäftliche emails zu verschlüsseln ?
Was ist sinnvoller : Inhalt- oder Transportverschlüsselung ?
Gibt es bezüglich der email-Verschlüsselung rechtliche Klarheit oder nur Empfehlungen von Datenschutzbehörden ?

Copyright © 2018-2021 id newmedia Stand Februar 2021

email-Verschlüsselung wird verwendet, um vertrauliche Informationen per email vom Absender zum Empfänger zu schicken. Möglich ist die Verschlüsselung zwischen den Endgeräten von Absender und Empfänger als Ende-zu-Ende-Verschlüsselung.

Ist laut DSGVO jetzt jede email zu verschlüsseln ?
Wie sieht es aus, wenn Sie eine email mit personenbezogenen Daten versenden ?
Müssen Sie nun jede email verschlüsseln ?

Prinzipiell gilt, daß die DSGVO in Sachen email-Verkehr nicht viel Neues mit sich bringt. Unternehmen wird schon nach dem Bundesdatenschutzgesetz empfohlen, das diese emails mit personenbezogenen Daten verschlüsseln - eine dahingehende Pflicht besteht aber bis heute nicht, d. h. : email-Verschlüsselung ist empfehlenswert, aber nicht verpflichtend.

Personenbezogene Daten liegen schon dann vor, wenn Sie in der email den Namen und die Anschrift des Empfängers nennen.

Aber auch andere Daten sind personenbezogen, beispielsweise :

- sexuelle Orientierung,
- ethnische Herkunft,
- politische Meinung,
- biometrische Daten,
- religiöse Überzeugung,
- Informationen über den Gesundheitszustand.

Verschlüsseln Sie eine email mit personenbezogenen Daten nicht, gehen Sie das Risiko ein, daß andere Personen die email unbefugt mitlesen, denn eine nicht verschlüsselte email ist wie eine Postkarte.

Geheimnisträger wie Rechtsanwälte, Steuerberater, Ärzte, Psychologen und Apotheker sollten jede email verschlüsseln, da sie sich sonst Risiken aussetzen. Zu dieser Einschätzung gelangt zumindest der Sächsische Datenschutzbeauftragte in seinem 8. Tätigkeitsbericht. Er stuft eine fehlende Verschlüsselung von emails in solchen Situationen ggf. als Straftat nach § 203 Strafgesetzbuch ein.

Für Unternehmen empfiehlt es sich schon aus naheliegenden Gründen, daß sie Dateien verschlüsseln. Verletzen sie datenschutzrechtliche Vorgaben, müssen sie die Datenschutzbehörden und die betroffenen Personen innerhalb von 72 Stunden darüber informieren. Versendeten sie die emails verschlüsselt, entfällt die Meldepflicht gegenüber der betroffenen Person.

Verschicken Sie verschlüsselte emails, ersparen Sie sich die Unannehmlichkeit daß Sie Ihre Kunden über eine sogenannte Datenpanne informieren müssen.

Sichere emails mit Inhalts- und Transportverschlüsselung
Sie möchten eine email mit personenbezogenen Daten verschlüsseln ? Dann sollten Sie die grundlegenden Verschlüsselungsmethoden und ihre Besonderheiten kennen :

→ https://de.wikipedia.org/wiki/E-Mail-Verschlüsselung

Bei der email-Verschlüsselung gibt es die *Transportverschlüsselung* und die *Inhaltsverschlüsselung*.

Transportverschlüsselung
Sie schicken eine sichere eMail durch einen „verschlüsselten Tunnel“. Die email liegt bei Absender und Empfänger entschlüsselt vor, auf dem Weg ist sie aber nicht durch Dritte lesbar. Der Client baut eine Verbindung zum Server auf. Der Server authentifiziert sich gegenüber dem Client mit einem Zertifikat. Der Client überprüft hierbei die Vertrauenswürdigkeit des X.509-Zertifikats und ob der Servername mit dem Zertifikat übereinstimmt. Optional kann sich der Client mit einem eigenen Zertifikat auch gegenüber dem Server authentifizieren. Dann schickt entweder der Client dem Server eine mit dem öffentlichen Schlüssel des Servers verschlüsselte geheime Zufallszahl, oder die beiden Parteien berechnen mit dem Diffie-Hellman-Schlüsselaustausch ein gemeinsames Geheimnis. Aus dem Geheimnis wird dann ein kryptographischer Schlüssel abgeleitet. Dieser Schlüssel wird in der Folge benutzt, um alle Nachrichten der Verbindung mit einem symmetrischen Verschlüsselungsverfahren zu verschlüsseln und zum Schutz von Nachrichten-Integrität und Authentizität durch einen Message Authentication Code abzusichern.

Inhaltsverschlüsselung
Die "Header"-Informationen der email, sprich Absender, Empfänger und Betreff, sind immer lesbar. Der restliche Inhalt ist verschlüsselt.

Client-basierte Lösungen haben den Nachteil, daß sie für viele Organisationen (Unternehmen, Vereine, …) zu komplex sind. Weil entsprechende IT-Infrastrukturen nicht vorhanden sind, ist die Versuchung groß, im Unternehmen ganz auf email-Verschlüsselung und Signatur zu verzichten.

Um die Nachteile der Client-basierten Verschlüsselung zu vermeiden, sind Server-basierte Lösungen das Mittel der Wahl. Die Arbeit der Verschlüsselung und Signatur wird dabei nicht von Clients und Anwendern, sondern im Hintergrund von Servern erledigt.

Bei einer Transportverschlüsselung ist die email nur auf dem Transportweg verschlüsselt. Sie befindet sich vor und nach dem Transport unverschlüsselt auf dem Server.

Das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) weist deshalb darauf hin, daß die TLS-Verschlüsselung ein „notwendiger Baustein“ für die elektronische Kommunikation ist. Sie ist aber kein Ersatz für eine Ende-zu-Ende-Verschlüsselung, sprich eine Inhaltsverschlüsselung. Um einen bestmöglichen Sicherheitsstandard zu gewährleisten, kombinieren Sie am besten **beide** Verschlüsselungsarten.

email-Verschlüsselung per TLS : was ist zu beachten ?
Sie verschlüsseln per TLS ? Dann wählen Sie eine nach dem aktuellen Stand der Technik sichere Verschlüsselung. Viele Absender denken, daß sie per TLS verschlüsseln was aber oft gar nicht zutrifft.

Und da Sie nach der DSGVO die Verschlüsselung personenbezogener Daten nachweisen müssen, kann es hier Probleme geben, → Art. 5 I, II DSGVO :

„Der Verantwortliche ist für die Einhaltung des Absatzes I verantwortlich und muss dessen Einhaltung nachweisen können („Rechenschaftspflicht“).“

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) weist darauf hin, daß eine TLS-Verschlüsselung erst ab der Version 1.2 zuverlässig ist. Ältere Versionen vor 1.2 sind also unsicher und verstoßen gegen den Datenschutz.

Ist ein TLS-Zertifikat erst einmal eingerichtet, läuft es normalerweise zuverlässig. In den folgenden Situationen ist die Verschlüsselung dann aber plötzlich wieder unsicher :

- Sie tauschen den entsprechenden Server aus;
- Sie oder eine Gegenstelle ändern die Konfiguration;
- Ihr Zertifikat verliert an Gültigkeit;
- die Empfängerstelle erkennt Ihr Zertifikat nicht an.

Denken Sie auch daran, daß eine TLS-Verschlüsselung richtig konfiguriert sein muß.

Viele Absender setzen den Haken bei „Optional TLS“. Die Verschlüsselungssoftware verschlüsselt die email dann aber nur, wenn dies möglich ist, ansonsten übermittelt die Software die email unverschlüsselt. Mit einem Secure email-Gateway (Security Appliance) kann Verschlüsselung flächendeckend umgesetzt werden. Da hier verschiedene Verschlüsselungsverfahren möglich sind, stellt das Security Gateway die verschlüsselte Kommunikation sicher.

Das Protokoll TLS eignet nicht für eine spontane und wechselnde email-Kommunikation, beispielsweise im B2C-Geschäft. Hier empfehlen sich eher Passwort-basierte Verfahren.

Welche Schnittstellen sollten Sie zur Verschlüsselung einrichten ?
Sie haben eine Transportverschlüsselung oder Inhaltsverschlüsselung eingerichtet ? Dann sind Sie rechtlich auf der sicheren Seite. Sie möchten nun eine ganzheitliche Verschlüsselungslösung für Ihr Unternehmen aufbauen ? Wir beraten Sie gerne …

Welche Probleme treten bei der email-Verschlüsselung in der Praxis auf ?
Komplizierte Lösungen taugen nicht viel, Ihre Mitarbeiter werden sie nicht benutzen.
Wenn Mitarbeiter emails über ihr Smartphone versenden muß die Verschlüsselung auch hier zuverlässig funktionieren. Es nützt nichts, wenn die Technik auf den Computern funktioniert, beim Versand über das Smartphone aber Sicherheitslücken bestehen. Wir beraten Sie gerne …

Beratung durch Experten
Unternehmen sollten sich durch IT-Experten beraten lassen. Denken Sie in diesem Zusammenhang unbedingt daran, daß Sie emails auch **archivieren** müssen.

Legen Sie die emails verschlüsselt ab, finden Sie diese nur schwer wieder. Die Suchfunktion benötigt den Klartext, der bei verschlüsselten emails nicht abrufbar ist. Würden wir Sie für eine Verschlüsselungslösung beraten, so würde diese auch Schnittstellen für Journal- und Archivsysteme bieten.

Sonderfälle und DSGVO-Fallen
Stellen Sie bei besonders sensiblen Daten eine hohe Geheimhaltung sicher. Es ist zwar wünschenswert, wenn Sie über Security Appliances Spam, Malware & Co. erkennen.

Allerdings sollten Sie vorrangig sicherstellen, daß niemand Kenntnis von Ihren personenbezogenen emails erlangt. Dazu eignet sich eine Ende-zu-Ende-Verschlüsselung (Inhaltsverschlüsselung).

Die gewählte Verschlüsselungslösung sollte auch die Cloud und mobile Endgeräte wie Smartphones und Tablets einbeziehen soll.

Beachten Sie, daß nicht nur Menschen emails versenden. Es gibt Applikationen, die emails automatisch versenden. In diesen emails befinden sich manchmal personenbezogene Daten, die geschützt werden müssen.

Dabei handelt es sich beispielsweise um automatisierte Rechnungen, Lieferscheine und Lohnabrechnungen. Die meisten Applikationen sind nicht darauf ausgelegt, emails zu verschlüsseln. Einige Anbieter bieten DSGVO-konforme Updates an, bei der Software anderer Anbieter müssen Sie manuell nachbessern.

Literatur

Bruce Schneier: Applied Cryptography. Protocols, Algorithms, and Source Code in C, Second Edition. 1996, ISBN 0-471-11709-9.
Niels Ferguson und Bruce Schneier: Practical Cryptography. 2003, ISBN 978-0-471-22357-3.
Bruce Schneier: E-mail Security. How to Keep Your Electronic Messages Private. 1995, ISBN 978-0-471-05318-7

Quellen
Auszugsweise nach Informationen von Sören Siebert, Rechtsanwalt, eRecht24
Wikipedia
DSGVO
Alles verwendete Bildmaterial : licensed by Vital Imagery Ltd. / id-newmedia

Zusammenfassung

Die email-Verschlüsselung ist immer empfehlenswert, sollten Sie personenbezogene Daten übermitteln.

Eine kombinierte Inhalt- und Transportverschlüsselung bietet eine gute Verschlüsselung.

Geheimnisträger, die emails unverschlüsselt versenden, gehen besondere Risiken ein.

Eine Verschlüsselung ist nutzlos, wenn diese nur am Desktop funktioniert. Die Verschlüsselung sollte für den konformen DSGVO-konformen email-Versand auch eine Cloud und mobile Endgeräte wie Tablets und Smartphones berücksichtigen.

Denken Sie daran, daß manche Ihrer Programme möglicherweise automatisch emails versenden.

Wählen Sie eine Verschlüsselung, die mit möglichst vielen Plattformen und Betriebssystemen kompatibel ist. Damit stellen Sie sicher, daß der Empfänger der email diese auch tatsächlich öffnen kann.

Verschlüsseln Sie emails, kann dieser Vorgang die Suchfunktion der Archivierung (zu der Sie ebenfalls verpflichtet sind) beeinträchtigen. Die Suchfunktion benötigt den Klartext von emails – ansonsten funktioniert sie nicht.

Nach einer Datenpanne müssen Sie die Datenschutzbehörden und die betroffenen Personen nach spätestens 72 Stunden über den Vorfall informieren. War die betroffene email verschlüsselt, entfällt die Meldepflicht gegenüber der(n) betroffenen Person(en).