Schindluder ausgeschlossen

Um einen schon abgenutzten Vergleich zu bemühen: E-Mail-Versand ist so, wie eine Postkarte zu verschicken – vertrauliche Informationen und persönliche Daten haben hier nichts zu suchen, nach der Datenschutzgrundverordnung kann ein Verstoß hohe Bußgelder nach sich ziehen. Weiter ausschließlich auf Briefpost zu setzen, ist im Zeitalter der Digitalisierung jedoch keine wirkliche Alternative. FACTS stellt hier verschiedene Dienste vor, die DSGVO-konforme Onlinekommunikation ermöglichen.

Manche Menschen finden es faszinierend, wenn ihr Kühlschrank Lebensmittel bestellt und ihre Uhr jede Körperregung auswertet, und es stört sie nicht, dass die Daten übertragen, gesammelt und ausgewertet werden. Andere fühlen sich durchleuchtet und fürchten Datenmissbrauch. Wer seine Daten freigebig veröffentlichen möchte, darf das tun, doch wer es nicht will, bekommt durch das Datenschutzgesetz das Recht auf eine gewisse Diskretion. Alle Datensammler müssen Vorgaben beim Umgang mit personenbezogenen Daten beachten: Durch die neue EU-Datenschutzgrundverordnung (DSGVO) werden diese Vorgaben etwas deutlicher beschrieben und der Verstoß wird erheblich höher bestraft.

DIE DSGVO BETRIFFT ALLE

Jedes Unternehmen hat es mit personenbezogenen Daten zu tun, deshalb geht die DSGVO alle etwas an. Viele wissen nur nicht, welche Daten damit gemeint sind. Personenbezogene Daten sind solche, mit denen eine Person identifiziert werden kann. Das muss gar nicht ein Datensatz mit Namen sein: Mittels Profiling können aus anonymen Daten durchaus Rückschlüsse auf eine Person gezogen werden. Sensible Daten befinden sich garantiert in der Personalverwaltung, in der Marketingabteilung und im Vertrieb. Dazu gehören neben Name, Geburtsdatum oder Adresse auch Kontoverbindungen oder Steuernummern sowie biometrische Daten. Weiterhin sind natürlich Daten schützenswert, die mehr über eine Person aussagen, beispielsweise über ihre Gesundheit. Auch genetische Daten – etwa die Hautfarbe oder die Herkunft – gelten als schützenswert.

Zu unterscheiden ist dabei, ob Max Mustermann für die Musterfirma arbeitet und seine ▸

KEINE CHANCE FÜR HACKER: *Eine E-Mail ausspähen ist leicht. Sie zu verschlüsseln ist umständlich. Es gibt jedoch Möglichkeiten, elektronische Sendungen einfach zu verschlüsseln und sicher zu machen.*

geschäftlichen Kontaktdaten auf der Unternehmenswebsite veröffentlicht sind oder ob Max Mustermann in der Musterstraße 1 in Musterstadt wohnt. Letzteres geht die Öffentlichkeit nichts an. Insofern sind Unternehmen stärker von der DSGVO betroffen, wenn ihre Kunden Privatpersonen sind (B2C). Doch auch im B2B-Geschäft sollte man sich in Acht nehmen.

Die DSGVO ist dafür da, dass mit diesen Daten kein Schindluder getrieben wird – was im Zeitalter von Big Data sicher ein notwendiger Schritt ist. Wie tief der Schutz in Unternehmensprozesse eingreift und ob die mitunter existenzbedrohenden Strafen bei Verstoß – bis 20 Millionen Euro oder vier Prozent des weltweiten Jahresumsatzes – angemessen sind, wird heiß diskutiert. Laut Kritikern wird zudem die Entwicklung neuer Technologien wie das Internet der Dinge, für die ständige Datenübertragung Voraussetzung ist, dadurch ausgebremst. Viele fragen sich zu Recht, ob denn auch die Daten derjenigen Menschen geschützt werden müssen, die ihr Leben in allen Details in den sozialen Medien zur Schau stellen. Doch geschützt werden sollen Menschen, die ihre Daten nicht preisgeben möchten und dazu durch fahrlässigen Umgang oder gezielte Verknüpfung auch nicht gezwungen werden sollen.

GROSSE VERANTWORTUNG

Schindluder könnte ein Unternehmen selbst treiben, indem es beispielsweise seine Kundendaten für Fremdzwecke zur Verfügung stellt, ohne das Einverständnis der betroffenen Personen eingeholt zu haben. Schindluder treiben auf jeden Fall Cyberkriminelle, die es auf personenbezogene Daten – etwa den Zugang zu Girokonten – abgesehen haben. Die DSGVO fordert von „Verantwortlichen und Auftragsverarbeitern" (bei Letzteren handelt es sich beispielsweise um Druckdienstleister oder Steuerberater) geeignete technische und organisatorische Maßnahmen für ein angemessenes Schutzniveau, also auch, den Zugriff durch Fremde abzuwehren. Dazu gehört unter anderem „die Pseudonymisierung und Verschlüsselung personenbezogener Daten" (Art. 32, Abs. 1 a). Dies ist absolute Pflicht und nicht nur eine Empfehlung für alle, die auf der sicheren Seite sein möchten. Sollte es zu Datenmissbrauch durch Dritte kommen, wird bei Unterlassung jeglicher Maßnahmen eine Mitschuld angerechnet.

Für alle gespeicherten Daten gilt zudem eine Rechenschaftspflicht: Der Verantwortliche muss die Einhaltung der Richtlinie in allen Facetten nachweisen können (Art. 5, Abs. 1 und 2). De facto ist das die Umkehrung der Beweislast, da ein

info Exkurs: Massen-E-Mails

Datenschutz im E-Mail-Verkehr ist nichts Neues. Schon seit der Datenschutznovelle von 2008 gilt der aktiv geäußerte Wunsch („Opt-in"), der vor allem verbietet, Menschen ohne ihr Einverständnis regelmäßig Werbung zuzuschicken, weil sich viele durch eine E-Mail-Flut belästigt fühlen. Ein voreingestelltes Häkchen, das bei einer Bestellung die Zusendung von Folgeangeboten erlaubte, sofern es nicht weggeklickt wurde („Opt-out"), ist also seitdem unzulässig. 2011 kam noch das „Double-Opt-in" hinzu, das verhindern soll, dass ein Roboter oder eine fremde Person beispielsweise eine Newsletterbestellung vornimmt: Auf die aktive Bestellung folgt eine E-Mail mit einem Link, über den die Bestellung – noch einmal aktiv – bestätigt wird. Damit hat der Versender einen Nachweis für die Einwilligung zur Nutzung einer persönlichen Adresse für den vereinbarten Zweck – und nur für diesen.

Darüber hinaus ist die Integrität der Empfänger beim Versand zu wahren. Im Jahr 2013 ging ein Fall durch die Presse, in dem eine Mitarbeiterin eines Handelsunternehmens eine Rundmail an Kunden verschickte – und alle Adressen in das „An"-Feld statt in „Bcc" eintrug. Mit diesem offenen Verteiler verstieß sie gegen § 3 des Bundesdatenschutzgesetzes. Das Bayerische Landesamt für Datenaufsicht verhängte aufgrund der unzulässigen Übermittlung personenbezogener Daten eine hohe Strafe gegen die Frau. In ähnlichen Fällen wurden Arbeitgeber in die Verantwortung genommen, da sie, so die richterliche Begründung, ihre Informationspflichten gegenüber den Mitarbeitern verletzt hatten.

Beschuldigter selbst seine Unschuld nachweisen muss, nicht der Kläger die Schuld. Noch dazu ist es unerheblich, ob ein Verstoß bewusst, durch kriminelles Einwirken von außen oder ganz und gar unbeabsichtigt verursacht wurde, denn es sollen ja Vorkehrungen gegen sämtliche Eventualitäten getroffen werden.

Sowohl die Nachweisbarkeit als auch die Empfehlung zur Verschlüsselung sind interessant für den E-Mail-Verkehr. Viele E-Mails werden in Massen verschickt und beinhalten Werbung oder interessante Informationen. Bei solchen Newslettern ist unbedingt darauf zu achten, die Empfängeradressen diskret zu behandeln – siehe Kasten auf Seite 30. Andere E-Mails im geschäftlichen Kontakt sind vom Inhalt her erheblich brisanter: Wenn wir einen Flug oder ein Hotelzimmer übers Internet buchen, wofür ein sicherer Kanal eingerichtet ist, erhalten wir eine Bestätigung per einfacher E-Mail. Mr. Cybercrime kann so herausbekommen, wann genau wir garantiert nicht zu Hause sind. Solche E-Mails gilt es von nun an zu verschlüsseln! Umgekehrt müssen Bewerbern Möglichkeiten eingeräumt werden, ihre Unterlagen über einen sicheren Kanal zu schicken, sofern die Personalabteilung keine Bewerbung per Post wünscht.

Verschlüsselungstechniken sind ganz und gar nicht neu. Sie konnten sich nur nicht durchsetzen, weil letztlich niemand verstanden hat, warum Bob einen öffentlichen Schlüssel herausrückt und Alice ihn für Nachrichten an ihn nutzt. Sobald irgendwelche Vereinbarungen zwischen den Kommunikationspartnern getroffen werden müssen, ist so eine Lösung nicht massentauglich: Wie soll man auf diese Weise die gesamte Geschäftskommunikation mit Bekannt und vor allem mit Unbekannt abwickeln? Ein weiteres Beispiel sind Verfahren wie E-Postbrief und De-Mail, die das Problem der ungeschützten Kommunikation endgültig lösen sollten. Es war eine aufwendige Registrierung eines jeden Teilnehmers notwendig, woraufhin er nur Menschen schreiben konnte, die ebenfalls Teilnehmer waren. Es war jedoch kaum möglich zu erfahren, wer Teilnehmer ist. Drei Hürden, die dem E-Postbrief das Genick gebrochen haben. Die De-Mail, höchststaatlich im De-Mail-Gesetz verankert und allen Behörden zur Nutzung verordnet, nimmt noch am Rennen teil.

FACTS stellt hier verschiedene sichere Dienste vor, die mehr oder weniger einfach zu handhaben und damit geschäftsalltagstauglich sind und bei denen Missbrauch durch Schindluder ausgeschlossen ist. Wobei „ausgeschlossen" natürlich immer nur heißen kann, dass der Aufwand in keinem Verhältnis zum Ertrag steht: Möglich ist alles, doch niemand wird wochenlang eine Verschlüsselung zu hacken versuchen, um eine Nachricht zu lesen, deren Inhalt möglicherweise vollkommen belanglos ist.

info Weitere Anbieter

Ähnlich wie die drei E-Mail-Lösungen funktionieren auch IncaMail der Swiss Post und Seppmail. Letzterer Anbieter hat auf unsere An- und Nachfrage nach Informationen jedoch nicht reagiert, die Swiss Post wiederum wendet sich ausschließlich an Konzerne, die Dokumente zu Tausenden versenden. Deshalb tauchen beide in der Übersicht nicht auf. Außerdem gibt es ECM-Anbieter, die – dem Gedanken des Sharings folgend – in ihrem System eine sichere Plattform anbieten, über die Unternehmen Dokumente untereinander oder sogar mit ihren Kunden „teilen" können. Da dies Bestandteile einer komplexen proprietären Lösung zum Dokumentenmanagement sind, hat FACTS darauf verzichtet, sie in die Übersicht aufzunehmen. Die in der Übersicht vorgestellten Dienste integrieren sich in jede bestehende Infrastruktur.

UNWISSENHEIT SCHÜTZT VOR STRAFE NICHT: *Strafbar macht sich auch, wer nicht ausreichend Sicherheitsmaßnahmen gegen Datendiebstahl getroffen hat.*

DIE ÜBERSICHT

Sieben Dienste für den sicheren Versand (siehe Tabelle auf der nächsten Seite):

- Cryptshare, RMail und die regify-Produkte bedienen sich der vorhandenen Mailprogramme und der bestehenden E-Mail-Adressen für den Transport. Die Verschlüsselung erfolgt auf Knopfdruck im Hintergrund, sodass Versender und Empfänger nicht mehr Aufwand haben als mit einer normalen E-Mail.
- Die drei Produkte von Mentana-Claimsoft, Tochterunternehmen von Francotyp-Postalia, sind ganz anders. Um „De-Mail" zu nutzen, müssen alle Beteiligten eine recht umständliche Identifizierung durchlaufen, bekommen eine spezielle Adresse und können nur untereinander kommunizieren. Das „Gateway" stellt eine gemeinsame Schnittstelle für verschiedene Dienste und zentralisiert so den De-Mail- und EGVP-Versand von allen im Unternehmen zugelassenen Clients, um den sicheren Prozess handhabbar zu gestalten. „FP-Sign" ist ein spezieller Dienst, der für komplexe, nicht alltägliche Geschäftsprozesse infrage kommt, beispielsweise wenn es viele Unterzeichner an verschiedenen Standorten für ein und dasselbe wichtige Dokument gibt.
- Kernstück der brieffabrik ist der bitkasten, der das digitale Äquivalent zum Briefkasten zu Hause ist: Die Sendungen aller Versender ▸

Anbieter	befine Solutions AG	Frama Deutschland GmbH	Mentana-Claimsoft GmbH
Produktbezeichnung	**Cryptshare**	**RMail**	**De-Mail Portal**
Verfahren	Kommunikationslösung, um vertrauliche E-Mails und Dateien beliebiger Größe sicher und nachvollziehbar auszutauschen. Dazu wird ein unternehmenseigener Server installiert, über den diese Daten ad hoc ausgetauscht werden können.	Plug-in zur Verschlüsselung von E-Mails. Auf jede Mail folgt ein „eingeschriebener Zustellungsnachweis" zur Überprüfung von Authentizität des Inhalts, Sende- und Öffnungszeiten sowie den verwendeten Verschlüsselungsmethoden. Viele Zusatzfeatures.	Portal zum Abrufen und Senden von De-Mails (geschlossenes System)
Verschlüsselungsart(en)	TLS, AES	Auto-TLS mit Secure PDF Fallback, AES265	TLS 1.2
Signatur und/oder Zeitstempel möglich?	Ja	Ja, auch „eVertrag"-Service	Jede De-Mail wird beim Senden signiert
Systemvoraussetzungen	Server: Windows- oder Linux-System. Virtuelle Appliances für VMware und Hardware-Appliances verfügbar Client: Browser, MS Outlook, IBM Notes	Office 365, Outlook, Gmail, RMail Inbox, RMail Web-App mit jedem Browser	Browser
Installationsvoraussetzungen	Eigene DMZ oder durch Drittanbieter gehostet	Plug-in für Mailprogramm	Keine
Registrierung/Authentifizierung/Log-in	Einmalige Überprüfung der E-Mail-Adresse durch Verifizierung (Zusendung eines Verifizierungscodes)	Einmalige Registrierung jedes Teilnehmers im RPortal. Jeder Nutzer kann seine Einstellungen individuell anpassen.	Alle Teilnehmer werden identifiziert. Normale Authentifizierung: Nutzername und Passwort. Hohe Anmeldung: mTAN oder nPA. Anmeldung mit Zertifikat.
Voraussetzungen beim Empfänger	Keine – ein Internetzugang und eine E-Mail-Adresse genügen.	Keine – ein Internetzugang und eine E-Mail-Adresse genügen.	Account eröffnen, Identifizierung durchlaufen
Sichere Antwort möglich?	Verschlüsselte Antwort kostenlos möglich	Verschlüsselte Antwort kostenlos möglich	Ja
Empfangs-/Lesebestätigung	Empfangsbestätigung	Verschlüsselter Zustellungsnachweis über Status, Zeitpunkt, außerdem Originalinhalt in verschlüsselter Form	Versand- und Eingangsbestätigung, persönlich, absenderbestätigt, abholbestätigt
Revisionssicherheit	Ja	Der Zustellungsnachweis enthält die Original-E-Mail inkl. aller Anhänge, die Fakten der Zustellung, sowie digitale Fingerabdrücke.	Ja, durch das De-Mail-Gesetz gilt De-Mail mit der Signatur als revisionssicher.
Produktvarianten	Nur Web-Oberfläche Web-Oberfläche + E-Mail-Integration Web-Oberfläche + E-Mail-Integration + Schnittstellen	RSign für komplexe Vertragsstrukturen und Workflows	Führen eigener Third-Level-Domain für De-Mail
Zusätzliche Features	E-Mail-Schutzklassifizierung (Klassifizierung ausgehender Nachrichten und Koppelung an bestimmte Vorgaben zum sicheren Versand), Versand von beliebig großen Dateien	Anhänge bis 1 GB, „eVertrag" für elektronische Vertragsabwicklung, automatisch Anhänge zippen oder in PDF konvertieren, Metadaten aus Anhängen löschen, Whaling-Erkennung	Nein
Automatisierungsmöglichkeiten	NET API, JAVA API, Kommandozeilen-Schnittstelle („Cryptshare Robot"). Dadurch Anbindung an eine Vielzahl von Systemen möglich.	Anbindung an bestehende ERP-Systeme möglich	Nein
Abrechnung	Lizenz mit Laufzeit von 12 oder 36 Monaten	Monatliche oder jährliche Volumentarife	Einzelsendung je nach gewählter Option
Zusatzkosten	Keine	Keine: alle Features inklusive	Erweitertes Postfach zur Aufbewahrung
Basispreis für eine Sendung	Wenige Euro pro Jahr für unbegrenzte Menge	Je nach Lizenz zwischen 0,01 € und 0,22 €	0,33 €
FACTS-Zusammenfassung	**Gut handhabbare Alternative zur normalen E-Mail mit breiten Integrationsmöglichkeiten zu einem günstigen Preis**	**Gut handhabbare Alternative zur normalen E-Mail. Tipp der Redaktion aufgrund des komplexen Zustellungsnachweises, der vielen nützlichen Features und des niedrigen, transparenten Preises**	**Alternative zur E-Mail, doch aufgrund der aufwendigen Identifikation und des geschlossenen Systems vergleichsweise schwer nutzbar**

Mentana-Claimsoft GmbH	Mentana-Claimsoft GmbH	output.ag	regify GmbH
Mentana Gateway für De-Mail, EGVP und beBPo	**FP-Sign**	**brieffabrik**	**regimail, regibill und regipay**
Gateway für die Integration der De-Mail-, EGVP- und beBPo-Funktionalitäten in das eigene Mailsystem (siehe Kasten auf Seite 34)	DTM-Verfahren zum sicheren und rechtskonformen Austausch und zur elektronischer Unterschrift von digitalen Dokumenten, Portallösung mit Postfachsystem	PDF- oder Word-Brief über einen Druckertreiber direkt in den digitalen Briefkasten (bitkasten) des Empfängers hochladen. Sobald der Empfänger die Sendung abgeholt hat, erhält der Versender eine Zustellungsbestätigung.	Nutzt klassische E-Mail als Transportweg für verschlüsselten Anhang. Die Verschlüsselung ist so automatisiert, dass der Nutzer sich nicht darum kümmern muss. Zu jeder Sendung wird eine nachweisbare Historie erstellt.
TLS 1.2, S/MIME	TLS 1.2	VPN/https	AES256; Unikat-Schlüssel je Einzeltransaktion
Signatur durch Provider, für Anhänge Signaturen, Zeitstempel und Verschlüsselung über MS Outlook	Von der einfachen bis zur qualifizierten Signatur, von der Intermediär- bis hin zur Fernsignatur	Ja	Ja, regify = register & certify
Server: Microsoft Windows, Microsoft Server, Linux auf Anfrage Client: lokaler E-Mail-Client	Browser-Portal-App, Integration durch API in Fachanwendungen	Druckertreiber, kostenloser Download über die Website der output.ag	Alle gängigen Betriebssysteme Lokaler Client, Portal, Apps (Android, IoS)
Mindestanforderung an die Hardware: Arbeitsspeicher: 4 GB, freier Festplattenplatz: 40 GB, freie USB-Anschlüsse für den Sicherheitstoken	Browser oder Anbindung in eigene Systeme durch API	Keine	Variabel: Cloud oder on Premise oder Mischformen
Geschäftskunde wird authentifiziert und spricht über Mailsystem Mitarbeiter an. Das Gateway identifiziert sich durch einen Token mit Zertifikat am De-Mail-Netz. Safe-ID beim EGVP.	Authentifizierung: mTAN, nPA, Videoident, persönlicher Ident, einmaliger Log-in durch Link, ansonsten Nutzername/Passwort	Keine Registrierung. Log-in per nPA oder Log-in-Daten	Teilnehmer melden sich selbst an bzw. können automatisiert angemeldet werden. Verschiedene Authentifizierungs-Niveaus mit Wahlmöglichkeit.
Account eröffnen, Authentifizierung, Third-Level-Domain, Installation Anmeldung EGVP (falls genutzt)	Keine – Empfänger bekommt Mail mit Link zum FP-Sign	Vorhandensein eines bitkastens/Authentifizierung über nPA	Vorhandensein eines regify-Accounts
Ja	Ja	Unidirektional	Ja, kostenlos für Privatpersonen
Versandbestätigung, Eingangsbestätigung, persönlich, absenderbestätigt, abholbestätigt	Sende- und Empfangsbestätigung ist signiert möglich	Ja, beides	Ja (register & certify)
Ja	Ja, durch Anbindung über die API oder Download der gezeichneten Dokumente mit Verifikationsprotokoll	Ja	Ja (register & certify)
Software-Gateway, Webservice	Integration in andere Fachanwendungen durch API	Integration in jegliche Prozessabläufe möglich	Die regify-Plattform ist die Basis für die Produkte regimail (E-Brief), regibill (E-Rechnung), regipay (E-Lohnbescheinigung), regigate, regibox, regichat.
Nein	Nachricht an Gegenzeichner, Delegationsfunktion für Unterschriften, automatisierter Workflow gestaltbar, MobileApp	Benachrichtigungsfunktion im bitkasten, Empfänger entscheidet, wie er seine Post erhalten möchte. Für den Empfänger ist der bitkasten kostenlos.	Für Rechnungsempfänger, Mitarbeiter, die regipays, oder auch Patienten, die Arztbriefe erhalten etc., ist die Rückantwort kostenfrei; regichat kann in Workflows eingebunden werden.
Archivschnittstelle zur Übergabe der Originalnachrichten an ERP/DMS für gesendete und empfangene Nachrichten, per Capture-Lösung auslesbar	Durch Einbindung der API und Gestaltung okumentenbezogener Workflows hohe Automatisierungsfunktion	Automatische Weiterleitung von Dokumenten. Empfänger verwaltet diese Funktion selbst im bitkasten. Integration in bestehende Systemlandschaft möglich.	Durchgängig für alle Produkte mittels SDKs
Gateway-Miete zzgl. De-Mail-Domain und Sendungen/Sendungsoptionen	Userbezogene und/oder transaktionsbezogene Abrechnung	Transaktionsbezogen	Flatrate bzw. auch Transaktionspreise bei Massenversand
Erweitertes Archiv	Ja	Keine	Keine
0,33 €	Basis-User inkl. 10 Dokumente/Monat 9,00 €	0,35 € für elektronische Zustellung	Ab 5,00 €/Monat für 500 Transaktionen
Sonderlösung: Schnittstelle für den Versand von vielen Clients und aus verschiedenen Anwendungen heraus	**Sonderlösung für Sendungen, die – unter Umständen von mehreren Personen – eine elektronische Unterschrift benötigen**	**Gute Alternative zur Portalzustellung von großen Unternehmen an ihre Endkunden, doch nicht für die alltägliche Korrespondenz geeignet**	**Gut handhabbare Alternative zur normalen E-Mail mit breiter Nutzungsmöglichkeit zu einem günstigen Preis**

info

EGVP und Nachfolger

EGVP steht für elektronisches Gerichts- und Verwaltungspostfach und ist eine elektronische Kommunikationsinfrastruktur für die verschlüsselte Übertragung von Dokumenten und Akten zwischen authentifizierten Teilnehmern von Gerichten und Behörden und ihrem Umfeld. Diesen Dienst gibt es seit 2004. Zurzeit wird er abgelöst durch die speziellen Verfahren beA, beN und BeBPo, die besonderen elektronischen Postfächer für Anwälte, Notare und Behörden, die auf der EGVP-Infrastruktur basieren.

▸ werden hier „eingeworfen“ und nur der eine Empfänger kann sie entnehmen. Damit kann er alle Einzelportale von Versicherungen oder TK-Anbietern an einer Stelle zusammenführen und muss sich nicht überall extra einloggen; nur antworten kann er von dort aus nicht. Wenn ein Empfänger seine Post nicht abholt, druckt die brieffabrik sie aus und lässt sie physisch von der Post zustellen.

VERSENDEN – UND MEHR

Nun zum Empfänger: Für den Erhalt einer De-Mail muss der Empfänger eine spezielle Adresse eingerichtet haben. Die Sendungen via Cryptshare, RMail oder regimail landen einfach im allgemeinen E-Mail-Postfach, wobei für regimail ein Account nötig ist, um den verschlüsselten Anhang zu öffnen; dieser lässt sich jedoch einfach einrichten. Aus dem bitkasten lädt sich der Empfänger nach dem Log-in seine Dokumente herunter.

Alle vorgestellten Verfahren bieten eine Empfangsbestätigung. Die von Mentana-Claimsoft und Frama sollen die Qualität eines Einschreiben-Rückscheins haben, wobei bei der RMail zusätzlich die Originalnachricht wiederhergestellt werden kann, sodass ihre Richtigkeit im Streitfall nachweisbar ist.

Über die Basisfunktion – elektronische Nachrichten sicher übertragen – hinaus gibt es bei manchen Diensten zusätzliche Funktionen, und zwar ganz unterschiedliche. Cryptshare bietet eine E-Mail-Schutzklassifizierung und die Möglichkeit, Dateien von beliebiger Größe zu verschicken. In die regify-Produkte reihen sich auch eine Chatfunktion und eine App. Bei der brieffabrik kann der Empfänger für jede Nachricht entscheiden, ob er sie elektronisch oder auf Papier erhalten möchte. In FP-Sign sind Einstellungen möglich, die eine Nachricht des Vertragsgegenzeichners erlauben, einen Vertreter zu ernennen, es lässt sich ein automatisierter Workflow gestalten und der Dienst per App nutzen.

In diesem Bereich „Zusätzliche Features“ hat jedoch eindeutig Frama die Nase vorn, denn RMail stellt ohne Aufpreis nützliche Optionen bereit, die den E-Mail-Versand bereichern. Der automatisierte „eVertrag“ ermöglicht einen schriftlichen Vertragsabschluss mit Unterschrift auf Distanz. Weiterhin kann eine RMail Dateien von 1 GB Größe verschicken: Das ist wie WeTransfer oder Dropbox, aber einfacher und verschlüsselt. Anhänge können per Klick wahlweise in ein PDF konvertiert oder gezippt werden, auch lassen sich die Metadaten aus MS-Office-Dokumenten entfernen. Interessant ist auch „SideNote“: Einer Nachricht kann für in Cc oder Bcc befindliche Empfänger eine Mitteilung beigefügt werden, die für die anderen nicht sichtbar ist. Für besondere Sicherheit von eingehenden E-Mails sorgt eine Whaling-Aufspürfunktion (siehe Kasten rechts). All diese Features sind standardmäßig enthalten und kosten nichts extra.

FAZIT

Wem es darum geht, DSGVO-konform zu kommunizieren, ohne jedes geschriebene Wort in Bezug auf vertrauliche und personenbezogene Daten auf die Goldwaage zu legen, ist mit jedem der vorgestellten Dienste durchaus gut bedient. Alle sind so gemacht, dass sie das Alltagsgeschäft nicht aufhalten, sondern sich so bedienen lassen wie die bewährten Kanäle; alle verschlüsseln unbemerkt im Hintergrund; alle lassen zudem die Wahl, eine unverfängliche Nachricht auf dem konventionellen – kostenlosen – Weg zu verschicken. Auch für die Nachweisbarkeit des Schriftverkehrs haben alle Anbieter eine Lösung.

In Sachen unkomplizierte Nutzung gibt es allerdings kein Smiley für De-Mail: Zwar ist sie durch das De-Mail-Gesetz als Einzige staatlich legitimiert und jede Behörde muss sie eigentlich unterstützen. Doch zum einen hat sie in der Bevölkerung so wenig Akzeptanz finden können wie individuelle aktive Verschlüsselung, was ihre Nutzung – gelinde gesagt – erheblich einschränkt. Zum anderen macht sie Halt vor Deutschlands Grenzen: Für internationale Korrespondenz ist sie gar nicht vorgesehen. Die brieffabrik wiederum ist interessant für die Zustellung von Rechnungen oder Mitteilungen an Endkunden und bietet einen erheblichen Mehrwert gegenüber üblichen Portallösungen, doch eignet sie sich nicht als Alternative für Korrespondenz, die auf eine Antwort abzielt.

Wer ein bisschen mehr Komfort haben möchte, wird sich wohl für RMail entscheiden: Die vielen erweiternden Möglichkeiten sind einfach überzeugend. Der einzige Wermutstropfen, den sicher nur wenige schlucken müssen: Es läuft nicht überall; wer beispielsweise unter Linux arbeitet oder Thunderbird für den E-Mail-Workflow nutzt, kann RMail (noch) nicht verwenden. Alle anderen können sich darüber freuen, dass sicher kommunizieren gar nicht viel kosten muss.

Anja Knies ■

info

Whaling

Whaling ist Phishing für Fortgeschrittene: Hier geht es ebenfalls um Identitätsdiebstahl, doch bei dieser Methode nutzen Cyberkriminelle nicht erfundene, sondern fremde Identitäten; sie gehen geschickter vor, um größere Geldsummen zu erbeuten.

RMail überprüft beispielsweise beim Antworten und Weiterleiten, ob die angezeigte E-Mail-Adresse tatsächlich der Absenderadresse entspricht, um gegebenenfalls vor einem möglichen Betrugsversuch zu warnen.