DOMINIQUE MAIER
Rechtsanwalt|Fachanwalt für Arbeitsrecht

Komprimiert und auf dem Präsentierteller:

Hinweise und Hilfestellung zur möglichst vertraulichen Kommunikation mit mir über das Internet

Stand 09.01.2020

Warum das Ganze?

Der sicherste Weg ist gewiss die persönliche Übergabe von Informationen. Dies ist allerdings aus verschiedensten Gründen nicht immer praktikabel und erfahrungsgemäß heute kaum noch üblich. Die Datenanlieferung erfolgt überwiegend online. Alles an Inhalten (Mail-Text, Anhänge), was nicht wirksam verschlüsselt wird, kann von unbefugten Dritten einer Postkarte gleich mitgelesen werden; leider nicht nur theoretisch, was bei der auf Vertraulichkeit angelegten Kommunikation zwischen Anwalt und Mandant ein Problem darstellt. Vertraulichkeit ist bei Klartextübermittlung via Internet ohne **Inhalts**verschlüsselung von vornherein nicht gewährleistet. Die reine **Transport**verschlüsselung zum Server Ihres Mail- oder Cloud-Providers verhindert nicht, dass E-Mails und Dateien in jeder Zwischenstation (z. B. E-Mail-Provider) im Klartext auf den Servern liegen. Dies gilt unabhängig davon, ob E-Mails mit Anhängen an mich übermittelt oder Dateien bei einem Anbieter (kostenlos bis 2 GB z. B. Wetransfer, Dropbox) für mich zum Download bereitgestellt werden. Wer Zugriff auf die temporären oder dauerhaften Lagerstätten der Daten hat und neugierig sowie entweder kriminell oder durch einen Gerichtsbeschluss legitimiert ist, kann einfach mitlesen. Sie merken es im Zweifel erst einmal nicht.

Selbstdatenschutz als Abhilfe:

Inhaltsverschlüsselung für die Internet-Brieffreundschaft mit mir als Ihrem Anwalt einmalig einrichten und glücklich sein! Geschützte Kommunikation online ist keine Raketenwissenschaft, man muss es nur einmal gemacht haben … und es sich zur Gewohnheit machen.

Warum nur „möglichst vertraulich“?

Ganz einfach. Einhundertprozentige Sicherheit ist kaum zu erreichen. Der Grad an Sicherheit hängt nämlich nicht nur vom Verschlüsselungsverfahren und meinen eigenen Sicherheitsvorkehrungen ab, sondern gerade auch von der in Ihrem Verantwortungsbereich vorgefundenen EDV-Umgebung nebst der zugehörigen Sicherheitsrichtlinien. Beispiel: Wenn Sie – im Falle der Nutzung von GnuPG, s. u. - Ihre EDV-Software (Betriebssystem, Virenschutz, Anwendungssoftware) nicht aktuell halten und Ihnen aufgrund eines Angriffs durch Ausnutzung einer Schutzlücke Ihr geheimer Schlüssel „geklaut“ wird; außerdem das dazu gehörende Schlüsselkennwort wegen fehlender Passwortrichtlinie „12345678“ lautet; oder das Schlüsselkennwort gar per Haftnotiz am Monitor „abgesichert“ ist: Dann kann der

verehrte lokale oder entfernte Angreifer jede Mail von mir – trotz Verschlüsselung – einfach mitlesen. Auf Ihre IT und die von Ihnen getroffenen organisatorischen Sicherheitsvorkehrungen habe ich keinen Einfluss.
Meine Ausführungen erheben keinen Anspruch auf Vollständigkeit. Es gilt das (auch auf die Anwaltsdienstleistung als solche übertragbare) Zitat von Bruce Schneier[1], einem Kryptographie-Experten aus den USA:

"Security is a process, not a product."[2]

À propos: Meine Richtlinie für sichere Kennwörter:
Mindestens 16 Stellen bestehend aus Großbuchstaben, Kleinbuchstaben, Ziffern und Sonderzeichen; Kombinationen aus Geburtsdaten, Namen oder Wörtern führen **nicht** zu einer wirksamen Verschlüsselung. Beispiel: Wjnl8,dhR!Adws,gb! Je mehr Zeichen und je "wirrer", desto sicherer, wobei das Beispielkennwort (gebildet aus der Eselsbrücke „Wer jetzt noch l8 (=lacht), der hat Reserven! Aber das wird schon, ganz bestimmt!") wegen der Veröffentlichung im Rahmen dieser Mandanteninformation schon „verbrannt" ist und nicht mehr verwendet werden darf. Empfehlenswerte Lektüre zu Kennwörtern:
http://www.1pw.de/brute-force.html

„Oh je!",
werden Sie sagen, wie soll ich mir das alles merken, bei den ganzen Passwörtern, die sich mit der Zeit ansammeln? Auch dafür gibt es Lösungen in Form von Passwort-Managern, bei denen man sich nur noch ein Kennwort für die Passwort-Datenbank merken muss, das aber schon den Anforderungen von oben entsprechen sollte, z. B.: https://keepass.info/

Ich stelle Ihnen nachstehend **drei Varianten** der Verschlüsselung vor. Sie selbst entscheiden aber, ob wir geschützt oder ungeschützt kommunizieren, **wobei ich die geschützte Kommunikation dringend empfehle. Bitte teilen Sie mir mit, ob und wenn ja: wie wir über das Internet kommunizieren sollen**. Bei den vorgestellten Lösungen (7-Zip, gpg4win, Signal) handelt es sich um Open Source Software, die sowohl im privaten als auch im kommerziellen Bereich kostenlos und frei nutzbar ist. Der Quellcode der Software ist für jeden einsehbar und auf Hintertürchen überprüfbar.
Vorteil der Varianten 2 und 3: Die Mitteilung von Kennwörtern ist nicht notwendig, was die Sicherheit erhöht.
Variante 2: Es müssen einmalig nur die nicht vertraulichen öffentlichen Schlüssel ausgetauscht werden. Den öffentlichen Schlüssel können (und müssen) Sie nach Belieben an Ihre Kommunikationspartner verteilen. Sie können ihn mir als Datei oder Textblock wie unten auch per E-Mail zukommen lassen, was anders als bei Kennwörtern absolut unbedenklich ist, weil der öffentliche Schlüssel nur zur VERschlüsselung geeignet ist (wie ein geöffnetes

[1] https://de.wikipedia.org/wiki/Bruce_Schneier
[2] http://www.hauke-laging.de/sicherheit/openpgp.html#warnung (dort gibt es auch SEHR vertiefte und engagierte Ausführungen zur Funktionsweise von GnuPG, bitte aber nicht abschrecken lassen).

Vorhängeschloss, das Sie mir in die Hand drücken und welches ich nur verriegeln, nicht aber wieder öffnen kann).

Variante 3:

Hier erfolgen die Schlüsselerzeugung und der Austausch der öffentlichen Schlüssel komplett im Hintergrund.

Bevor Sie zur Tat schreiten, klären Sie im Unternehmensumfeld bitte, ob Sie zur Installation der Anwendungen befugt sind. Im Zweifel fragen Sie den Systemadministrator.

Ich bin verwirrt! Welche Variante empfehlen Sie mir?

- Unerfahrene Anwender greifen zu den Varianten 1 oder 3.
- Erfahrene Anwender greifen zu der Variante 2.

Variante 1 (Dateien mit Packgrogramm verschlüsseln)

7-Zip (https://www.7-zip.org/) ist eigentlich ein Packprogramm: Man hat eine oder mehrere Dateien, die man in einer Datei (sog. Archiv- oder Container-Datei) zusammenpackt. Der Vorteil dabei ist, dass ein Archiv üblicherweise eine geringere Speichergröße aufweist, als die unverpackten Einzel-Dateien. Vorteil zwei ist: Man kann die Archiv-Datei gegen neugierige Blicke schützen, indem man das ganze Dateien-Paket gleichzeitig verschlüsselt. Eine Anleitung für Windows finden Sie unter:
https://www.ra-maier.com/wp-content/uploads/2018/05/Anleitung_zur_Benutzung_von_7-Zip_unter_Windows.pdf
Als Archivformat 7z wählen und als Verschlüsselungsverfahren AES-256. Das Kennwort der Datei bitte nicht per E-Mail mitteilen. Das wäre ungefähr so, als ließen Sie mir durch einen Ihnen nicht näher bekannten Boten ein abgeschlossenes Behältnis zukommen, wobei Sie dem Boten der Einfachheit halber gleich den Schlüssel mit in die Hand drücken. Getrennter Versand durch zwei E-Mails ist genau so sinnlos. Der geneigte Angreifer greift dann eben beide Male beherzt zu und hat alles, was er benötigt (verschlüsselte Datei und das Kennwort).

Bis 10 MByte: E-Mail-Versand:

Beim E-Mail-Versand der Archiv-Datei bitte beachten: Der E-Mail-Inhalt wird anders als der mit 7-Zip verschlüsselte Dateianhang im Klartext übermittelt. Diese Variante ist **nicht** dazu geeignet, vertrauliche Informationen im E-Mail-Text zu schützen. Es empfiehlt sich, vertrauliche Mitteilungen ebenfalls als mit 7-Zip verschlüsseltem Anhang zu übermitteln und das Betreff sowie den eigentlichen Text der E-Mail sehr unverfänglich zu halten.

Für alles, was größer als 10 MByte ist: Online-Speicher:
Wenn Sie die Archiv-Datei per Cloud auf den Weg bringen möchten, kann ich Ihnen einen Link zum Hochladen übermitteln. Kurzer Anruf oder kurze E-Mail genügen. Oder Sie nutzen Ihren eigenen Cloud-Dienst und lassen mir den Download-Link zukommen. Das Kennwort der Archiv-Datei bitte auch bei Nutzung Ihrer Cloud **nicht** als unverschlüsselte E-Mail zusenden.

Variante 2 (GnuPG)

Ich stelle nachfolgend nur die GnuPG-Lösung vor, da die Schlüsselpaare außer ein wenig Investition von Zeit nichts kosten. Ich biete aber auch das S/MIME-Verfahren an, die Zertifikate sind in der Regel jedoch kostenpflichtig. Meinen öffentlichen S/MIME-Schlüssel finden Sie auf meiner Hompepage: https://www.ra-maier.com/nuetzliches/

Bis 10 MByte: E-Mail-Versand:

a) Vorab ein **Hinweis zur Efail-Schwachstelle**: Die unten dargestellte Implementierung der Verschlüsselung in E-Mail-Programmen – nicht die Verschlüsselung selbst – ist angreifbar. Beim unten dargestellten GnuPG-Verfahren ist aus Sicherheitsgründen zu empfehlen, im E-Mail-Programm alle aktiven Inhalte zu deaktivieren. Dazu zählt die Ausführung von html-Code und das Nachladen externer Inhalte, die oftmals aus Design-Aspekten erlaubt sind. Ich verweise auf https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2018/efail-schwachstellen_15052018.html und auf https://www.bsi-fuer-buerger.de/BSIFB/DE/Service/Aktuell/Informationen/Artikel/efail_schwachstellen.html. Halten Sie außerdem das E-Mail-Programm und das Plug-in zur Ver- und Entschlüsselung stets auf dem neuesten Stand.

b) E-Mail-Verschlüsselung unter Windows[3] einrichten:
http://www.german-privacy-fund.de/e-mails-verschlusseln-leicht-gemacht/
Verlieren Sie den geheimen Schlüssel des erzeugten Schlüsselpaares, ist eine Entschlüsselung durch Sie nicht mehr möglich. Befolgen Sie daher während der Einrichtung am besten den Rat, eine Sicherungskopie anzulegen und bewahren Sie diese sicher auf einem externen Datenträger auf. Gleiches gilt für das Kennwort zum geheimen Schlüssel und Ihr Widerrufszertifikat, das Sie bitte in jedem Falle anlegen.
Wichtig: Bevor wir jetzt möglichst vertraulich kommunizieren können, müssen wir uns – einmalig! - gegenseitig davon überzeugen, dass die öffentlichen Schlüssel vom jeweiligen Brieffreund stammen. Dies geschieht durch Überprüfung der Fingerabdrücke (Zahlen – und Buchstabenreihe) der Schlüssel. Lassen Sie sich die Eigenschaften meines öffentlichen Schlüssels mit der von Ihnen verwendeten Software anzeigen und rufen Sie mich an. Wenn der bei Ihnen angezeigte Fingerabdruck mit dem von mir vorgelese-

[3] Mac OS kann ich nicht (Lösung vielleicht hier: https://gpgtools.org/) und wer Linux nutzt, der benötigt mit hoher Wahrscheinlichkeit keine Hilfestellung ;-) (der Vollständigkeit halber Lösung für Ubuntu hier: https://wiki.ubuntuusers.de/Thunderbird/Enigmail/), Android (Smartphone) kann auch gnupg-Verschlüsselung, hier heißen die Stichworte für Google K9-Mail und Openkeychain,
Eine weitere gute Anleitung für alle Betriebssysteme mit prägnanter Info-Grafik gibt es auf Deutsch hier: https://emailselfdefense.fsf.org/de/windows.html

nen Fingerabdruck übereinstimmt, steht der vertraulichen Brieffreundschaft nichts mehr im Wege. Warum ist das so? Jeder kann sich für die E-Mail-Adresse info@ra-maier.com einen GnuPG-Schlüssel erzeugen und verwenden. Daher muss man einmalig sicherstellen, dass der öffentliche Schlüssel seines Gegenübers auch tatsächlich seinem Gegenüber gehört und nicht einem Spitzbuben, der nur so tut als ob, um vertrauliche Korrespondenz abzugreifen (neudeutsch nennt man das „Man-In-The-Middle-Angriff").

c) E-Mail-Verschlüsselung verwenden[4]:
Versand: https://support.mozilla.org/de/kb/nachrichten-digital-signieren-und-verschlusseln#w_eine-digital-signierte-undoder-verschlaksselte-e-mail-versenden
Empfang: https://support.mozilla.org/de/kb/nachrichten-digital-signieren-und-verschlusseln#w_eine-digital-signierte-undoder-verschlaksselte-e-mail-lesen

d) Die Betreffzeile der E-Mail wird NIE verschlüsselt übertragen, sondern nur der E-Mail-Text und die Anhänge. **Vertrauliche Informationen gehören somit nicht in das Betreff-Feld**. Im Klartext werden auch die sonstigen Meta-Daten im Internet übertragen wie Absender und Empfänger der E-Mail, Serverkennungen. Bitte vergewissern Sie sich vor dem Versenden, dass die Verschlüsselung der Mail und etwaiger Anhänge entsprechend aktiviert ist.

Für alles, was größer als 10 MByte ist: Online-Speicher:
Dateien vor dem Upload verschlüsseln: Dies geht mit dem Tool mit GPA (Bestandteil von gpg4win). GPA → Dateiverwaltung → Öffnen (hier die Datei/en auswählen) → Verschlüsseln (mit Ihrem eigenen und meinem öffentlichen Schlüssel). Es wird eine .gpg-Datei erstellt, die wie ein Container mit Vorhängeschloss alle von Ihnen ausgewählten Dateien enthält. Das Vorhängeschloss können nur Sie oder ich öffnen. Verschlüsseln Sie nur mit meinem öffentlichen Schlüssel und nicht mit Ihrem eigenen, kann nur ich das Vorhängeschloss öffnen.
Alternativ, wenn GpgEX als Bestandteil von gpg4win installiert ist: Windows-Explorer → zu verschlüsselnde Dateien markieren → Rechtsklick → Mehr GpgEX Optionen → Verschlüsseln. Es wird wie oben eine .gpg-Datei ausgeworfen.
Wenn Sie die gpg-Datei per Cloud auf den Weg bringen möchten, kann ich Ihnen einen Upload-Link übermitteln. Kurzer Anruf oder kurze E-Mail genügen. Oder Sie nutzen Ihren eigenen Cloud-Dienst und lassen mir den Download-Link zukommen.

Mein öffentlicher Schlüssel,
der für die Verschlüsselung von E-Mails/Dateien an mich benötigt wird steht als **Download** in Form einer .asc-Datei von meiner Homepage unter https://www.ra-maier.com/wp-content/uploads/2017/09/Oeffentlicher-gpg-Schluessel-info-at-ra-maier.com.asc zur Verfügung

[4] Funktioniert auch mit dem **eigenen Mailprogramm** oder **Webmail** über einen Umweg: Mail mit eigenem Mailprogramm verfassen. Text markieren und kopieren. Den Text im gpg4win-Tool GPA in das Fenster „Zwischenablage" einfügen. Auf „verschlüsseln" klicken. Das Ergebnis markieren und kopieren, um den unverschlüsselten E-Mail-Text im Mailprogramm durch den verschlüsselten E-Mail-Text zu ersetzen. Das Kauderwelsch kann ich dann nach Empfang der Mail mit meinem geheimen Schlüssel lesbar machen. Für Nutzer von **Outlook** enthält gpg4win ein Add-In namens **GpgOL**.

Variante 3 (Signal)

Signal ist ein Messenger wie WhatsApp: https://de.wikipedia.org/wiki/Signal_(Messenger). Es gibt aber auch eine Desktop-Variante für Ihren Computer. Sie können Anhänge bis zu 100 MB in einer Nachricht an mich versenden. Ende-zu-Ende-verschlüsselt. Der Quellcode ist offen und einsehbar. Die Nutzung ist sowohl im privaten und geschäftlichen Verkehr kostenlos.
Nur drei Schritte sind notwendig: 1. Signal auf Ihrem Smartphone installieren (Google Play Store, Apple App Store). 2. Signal herunterladen (https://signal.org/download/) und auf Ihrem Desktop-Computer installieren. 3. Über das Einstellungsmenü auf dem Smartphone Ihren Desktop-Computer als verknüpftes Gerät hinzufügen. Sie benötigen noch meine Mobilfunknummer, damit Sie Nachrichten an mich versenden können. Bitte kurz anrufen, dann verrate ich sie Ihnen. Bei dieser Gelegenheit können wir noch – einmalig! - die Sicherheitsnummern abgleichen, um uns gegenseitig davon zu überzeugen, dass sich hinter Kontakteintrag in Signal auch tatsächlich der jeweilige Brieffreund verbirgt.

Lob, Kritik, Anregungen und Hinweise auf veraltete Links sind willkommen!