Im Gespräch

Die Krux mit E-Mails

Kein anderes schriftliches Kommunikationsmittel hat sich sowohl im privaten als auch im beruflichen Alltag so stark etabliert wie die E-Mail. Über 300 Mrd Nachrichten werden täglich rund um den Globus verschickt. Doch wie vertraulich sind diese Inhalte, wenn die Nachrichten am unverschlüsselten Transportweg zwischen den einzelnen Mail-Servern abgefangen und gelesen werden können? In Bezug auf die Verwendung durch berufliche Geheimnisträger erscheint das höchst problematisch. Mag. *Markus Dörfler,* LL.M., der Datenschutzbeauftragte der RAK Wien, gibt Auskunft.

2022/210

Warum erfüllt die herkömmliche E-Mail die Anforderungen an eine vertrauliche Kommunikation nicht?
Eine E-Mail krankt prinzipiell an fünf Punkten: Ich weiß nicht, wer der Absender ist. Ich weiß nicht, wer der Empfänger ist. Ich weiß nicht, ob die E-Mail überhaupt angekommen ist. Ich weiß nicht, ob die E-Mail verändert worden ist. Ich weiß nicht, ob die E-Mail mitgelesen wurde.
Die technische Spezifikation des E-Mail-Systems stammt aus den 1970er-Jahren. Ursprünglich gab es keine Verschlüsselung und es gab nur wenige Menschen, die senden und empfangen konnten. Diese fünf Punkte waren daher in der Vergangenheit irrelevant. Jetzt setzt man neue Techniken auf das alte System auf. Die eingangs erwähnten fünf Punkte versucht man in den Griff zu bekommen, aber: Sicher ist das alles nicht.

Das anwaltliche Berufsrecht setzt aber hohe Maßstäbe an die Verschwiegenheitspflicht.
Als Rechtsanwälte sind wir zur Verschwiegenheit verpflichtet und in diesem Rahmen stellt sich die Frage, ob eine unverschlüsselte normale E-Mail diesem Kriterium entspricht.

Bedeutet das, dass Rechtsanwälte E-Mails gar nicht mehr verwenden dürfen?
Diese Frage kann ich so nicht beantworten, da es auf den Einzelfall ankommt. Bei der Verwendung einer unverschlüsselten E-Mail können Haftungsproblematiken entstehen. Wenn eine unverschlüsselte E-Mail verwendet wird, muss dem Mandanten zumindest das Risiko bewusst sein. Ihm muss klar sein, dass diese fünf Punkte nicht gewährleistet sind, wenn er eine unverschlüsselte E-Mail an den Rechtsanwalt sendet oder von ihm empfängt.

Das System muss in den Work-Flow passen.

Kann der Mandant seinen Rechtsanwalt von der Verschwiegenheitspflicht entbinden und explizit verlangen, dass mittels E-Mails kommuniziert wird?
Soweit ich weiß, gibt es dazu keine Entscheidungen. Ich würde allerdings meinen, dass der Mandant sich sehr wohl bewusst auf dieses Thema einlassen kann. Wenn es sich um einen mündigen Bürger handelt, wird er in Kenntnis der Sachlage dieses Risiko akzeptieren können. Er könnte ja beispielsweise auch die Kommunikation mit dem Rechtsanwalt veröffentlichen.
Die jüngsten Chat-Vorfälle in der Politik beweisen eines: Wenn Daten unverschlüsselt abgelegt werden, können sie ungewollt zum Vorschein kommen und Probleme für Menschen bedeuten, die gar nicht in der Kommunikation dabei waren. Schon aus diesem Grund muss ein Rechtsanwalt Sicherheitsmaßnahmen ergreifen, sodass die E-Mails nicht von jedermann mitgelesen werden können.

Aus diesem Grund hat der ÖRAK gemeinsam mit Partnern die Plattform context entwickelt, über die ein vertraulicher Dialog auch im Internet möglich ist.
Für den sicheren Datenaustausch gibt es unterschiedliche Systeme. Auch der ÖRAK hat ein solches System entwickelt, das ein Hauptproblem in den Griff bekommen möchte: die Benutzbarkeit durch die breite Masse. Zwar gibt es viele solcher Produkte am Markt, das größte Problem ist jedoch die Einbettung in den Work-Flow. Das System muss einerseits in die IT-Landschaft des Rechtsanwalts integriert sein und andererseits für den Mandanten so einfach nutzbar sein, dass er von überall zugreifen kann, auch von einem mobilen Endgerät.

Was muss auf Rechtsanwalts-Seite gegeben sein, außer die Integration in die Anwalts-Software, die bei context möglich ist?
Der wesentliche Punkt ist: Das System muss in den Work-Flow hineinpassen. Ein Konzipient oder ein Assistent schreibt Texte, die durch den Rechtsanwalt freigegeben werden. In der Kanzleisoftware müssen diese so abgespeichert werden, dass ersichtlich ist, was der Rechtsanwalt wann wem geschickt hat. Die Nachricht muss auch gegebenenfalls ein berechtigter Dritter, der an der ursprünglichen Erstellung nicht beteiligt war, nachvollziehen und lesen können. Bei E-Mail-Verschlüsselungen besteht das Problem, dass möglicherweise berechtigte Dritte nicht mehr zugreifen können, verteilte Schlüssel notwendig sind etc. Dementsprechend ist es sinnvoll, dass eine Lösung implementiert ist, die den technischen Prozess so vorsieht, dass alle Beteiligten, die zugreifen müssen, auch zugreifen können, aber sonst niemand.

Technisch löst context die Problemstellung der Vertraulichkeit so, dass nicht die Nachricht selbst übermittelt wird, sondern der Empfänger vom Erhalt einer Nachricht verständigt wird und diese selbst über eine verschlüsselte Verbindung von einer gesicherten Plattform abruft. Sind damit alle Sicherheitsbedenken zerstreut?
Es ist ein Kompromiss zwischen Sicherheit und Komfort, der aus meiner Sicht wohl ausreichend ist. Normalerweise hätte ich das Problem, das Gegenüber authentifizieren zu müssen. Im besten Fall, das wäre bei der Handy-Signatur so, habe ich eine Zertifizierungsstelle, die mir die Identität einer Person bestätigt und ich somit weiß, dass die Signatur von der Person stammt, die sie behauptet zu sein. Im Rahmen der anwaltlichen Praxis ist das zumeist nicht notwendig. Ich sehe mein Gegenüber und trete in ein Mandatsverhältnis ein. In vielen Fällen lässt man sich dann keinen Ausweis zeigen, sondern sorgt dafür, dass diese Person eine Benutzerkennung erhält. Die Erstbenachrichtigung bei context erfolgt über E-Mail und dann muss man sich einloggen und ein Passwort vergeben.

Genau, oder per SMS einen Token anfordern.
Wenn also der eine Kommunikationsweg, die E-Mail, kompromittiert ist, besteht zumindest ein zweiter Faktor. Es müssen beim ersten Mal also zwei Kommunikationswege gleichzeitig benutzt werden. Das führt dazu, dass ich ein deutlich höheres Sicherheitssystem nutze, ähnlich wie es heute bei Banken oder Versicherungen üblich ist. Dort erfolgt meist eine Authentifizierung über SMS oder eine App. Ob ich das bei einer permanenten Kommunikation benötige, wage ich zu bezweifeln. Context sorgt dafür, dass ich nicht über einen ungesicherten, von mir nicht kontrollierbaren E-Mail-Server kommuniziere und damit sicherstelle, dass ein Systemadministrator nicht mitlesen kann. Das ist aus meiner Sicht um ein Zigfaches sicherer als die Kommunikation über E-Mail.

Wie viel Geld ist ein Rechtsanwalt bereit, für sichere Kommunikation auszugeben?
Wenn ich mir ansehe, wie viel Geld wir jährlich in Sicherheit hineinstecken müssen – da rede ich von Sicherheitsupdates, die eingespielt werden müssen, Spamfilter, Virenfilter, Firewalls, die immer auf dem aktuellen Stand gehalten werden müssen, und für die pro Person und Jahr mehrere hundert Euro anfallen – dann muss mir die sichere Kommunikation wohl wenige hundert Euro pro Jahr wert sein.

In welchem Ausmaß muss eine Rechtsanwaltskanzlei für die Absicherung ihrer eigenen IT-Infrastruktur Sorge tragen, Stichwort Passwortschutz, Stichwort Daten-Back-up, Stichwort Cloud?
Wir haben mehrere mögliche Angriffspunkte, bei denen Datensicherheitsmaßnahmen ergriffen werden müssen. Da ist zunächst alles, was mit dem Benutzer zu tun hat: das Endgerät, das mobile Endgerät und der Arbeitsplatz. Genauso wie

ich Sorge zu tragen habe, dass es ein Schloss beim Eingang gibt, ist es notwendig, dass ich den Arbeitsplatz verschlüssle, mobile Endgeräte verschlüssle und mit einem Passwortschutz versehe. Ich brauche Virenscanner und ein Mobile-Geräte-Management, das bei großen Software-Anbietern, die eine Multi-User-Verwaltung anbieten, meist inkludiert ist. Die Geräte sind also über die Ferne zumindest löschbar. Ein großes Thema besteht bei der Infrastruktur, also den Netzwerken und Servern. Da werde ich Updates einspielen müssen, eine Wartung durchführen, Backups durchführen [...] Ich brauche eine Firewall, Spam-Filter, Viren-Filter [...].

Ohne IT-Dienstleister geht es heute nicht mehr.

Also eine ganze Menge. Optimalerweise habe ich einen IT-Dienstleister, der mir all das im Paket anbietet?
Ohne IT-Dienstleister wird es wohl nicht gehen. Ich behaupte, dass es in Österreich nicht viele Rechtsanwälte gibt, die es schaffen, das selbst zu administrieren. Externe Dienstleistungen wie zB von Clouds sind wieder ein eigenes Thema. Wenn ich heute zu einem Cloud-Dienstleister gehe, muss ich dafür Sorge tragen, dass dieser Dienstleister weiß, dass ich Rechtsanwalt bin und dass bei einer Hausdurchsuchung beim Cloud-Dienstleister meine E-Mails anders zu behandeln sind. Daher ist es von Vorteil, jemanden zu beauftragen, der die Rechte und Pflichten von Rechtsanwälten kennt und darauf Rücksicht nimmt.

Wir haben bislang über schriftliche Kommunikationsmittel gesprochen. Wie sieht es mit dem Telefon aus, ist das nicht auch ein großer Risikofaktor?
Das Mithören von Telefonaten ist technisch möglich, auch bei einer Mobilfunkverbindung und auch bei VoIP. Das Risiko, dass hier etwas passiert, ist aus meiner Sicht aber relativ überschaubar. Die Telefonie läuft über Provider und eine Speicherung dieser Information wäre aufwendiger. Die E-Mail ist sowieso gespeichert, da kann man zu jeder Zeit nachschauen. Beim Telefonat müsste man aber in Echtzeit alles mitschneiden und transkribieren. Das Risiko, den Kommunikationspartner nicht zu kennen, ist beim Telefon auch nur bedingt gegeben, weil durch die Kommunikation selbst ja bereits eine Identifikation stattfindet und man den Anderen in der Regel bereits an der Stimme erkennt.

Es wird davon gesprochen, dass Daten das neue Gold wären. Welche Tipps haben Sie für Privatpersonen in Bezug auf den Umgang mit den eigenen persönlichen Daten?
Es gibt ein paar Kleinigkeiten, mit denen man wesentlich leichter durchs Leben kommt. Das hat ganz viel mit Hausverstand zu tun. Wenn ich zB eine E-Mail-Nachricht bekomme, dass mein Konto gesperrt wurde, muss ich mir ernsthaft die Frage stellen, ob mir meine Bank diese nicht ganz unwesentliche Information wirklich einfach so, in einer möglicherweise schlecht formatierten E-Mail senden würde? Diese Phishing-Mails zielen darauf ab, dass man in Stress gerät. Ich brauche aber nie in Stress geraten. Wenn es wirklich wichtig ist, bekomme ich nicht einfach eine E-Mail, die mich auffordert, mich einzuloggen.
Wenn ich mich im Internet bewege, gilt auch hier wieder, mit Hausverstand online zu bestellen. Wenn ich auf einer Plattform bestelle, bei der ich noch nicht Kunde bin, suche ich auf der Seite das Impressum. Wenn nicht ganz klar ist, wer mein Vertragspartner ist, ist es sicherlich kein gutes Angebot. Wenn jemand seriös ist, hat er gewisse Informationen zu seiner Person auf seiner Website. Ein einfacher Telefonanruf genügt oft, um zumindest sicherzugehen, dass sich auf der anderen Seite ein Mensch meldet.
Ein letzter Punkt: Wir glauben alle, dass wir wahnsinnig wichtige Informationen haben, die wir der Menschheit preisgeben wollen. Posten Sie nicht irgendwelche Dinge zu Ihrer Person – das hilft beim Phishing!

Also Finger weg von Social Media?
Nein gar nicht, aber wenn ich etwas poste, muss ich mir gut überlegen, was ich poste und warum ich es poste. Wenn ich Urlaubsfotos poste, ist nichts Verwerfliches daran, wenn ich sicherstelle, dass das nur von Personen gesehen werden kann, von denen ich möchte, dass sie es sehen. Und eben nicht im öffentlichen Profil, sodass der Einbrecher weiß, dass niemand daheim ist.
Wenn trotzdem einmal etwas passiert, nicht ärgern, sondern daraus lernen.

Danke für diese Tipps und das Gespräch.

Mag. *Markus Dörfler*, LL.M., geb 1979 in Graz, verheiratet, ein Kind; studierte Rechtswissenschaften in Graz und Linz sowie Rechtsinformation in Wien, Rechtsanwalt seit 2012, 1999 Gründer des Synaptic Networks, Datenschutzbeauftragter der RAK Wien, Trainer am BFI Wien

Fotos: Werner Himmelbauer