bepartners
bödecker ernst & partner

beleuchtet

16. Juli 2013

Angriff auf die Vertraulichkeit

Unsere Serviceleistungen für eine vertrauliche elektronische Kommunikation

Die jüngsten Enthüllungen vor allem des Whistleblowers Edward Snowden führen uns vor Augen, dass unsere vertrauliche Kommunikation über das Internet nicht nur technikbedingt-theoretisch, sondern tatsächlich gefährdet ist. Diese neuen Erkenntnisse haben große Bedeutung für den Austausch zwischen Mandant und Berater. Wir möchten die aktuelle Debatte zum Anlass nehmen, Ihnen unsere Serviceleistungen für eine vertrauliche Kommunikation und Datenübertragung in Erinnerung zu rufen. Auf den folgenden Seiten erläutern wir, wo das Problem der unverschlüsselten E-Mail-Kommunikation liegt – und wie wir das Sicherheitsniveau unserer Kommunikation und unseres Datenaustauschs durch den Einsatz einfacher Mittel deutlich verbessern können.

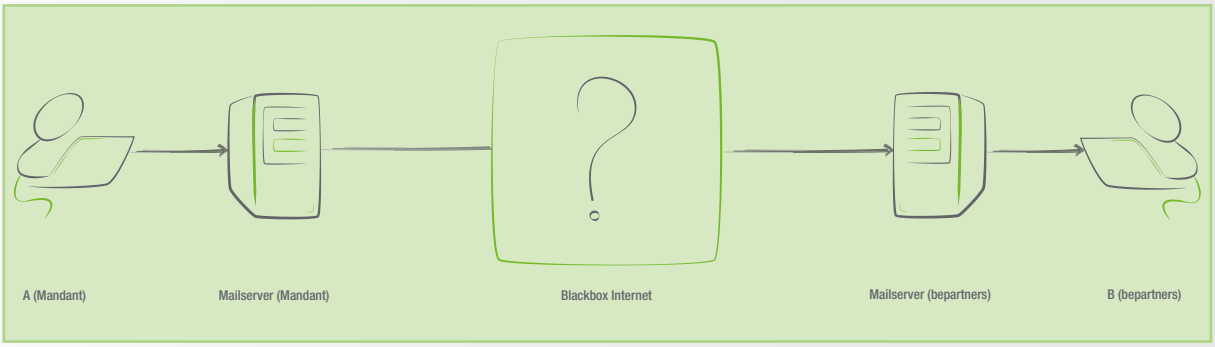
Das Problem: Die unverschlüsselte E-Mail

Die unverschlüsselte E-Mail ist leider immer noch Standard in der geschäftlichen Korrespondenz; obwohl sie keine Vertraulichkeit gewährleisten kann. Sie haben vermutlich bereits einmal den Vergleich mit einer Postkarte gehört: Eine unverschlüsselte E-Mail kann wie eine Postkarte auf ihrem Übertragungsweg von jedem mit Zugriff auf die Netzwerkinfrastruktur gelesen werden. Dies gilt sowohl für den Text der E-Mail selbst als auch für mögliche Dateianhänge. Dass eine solche Überwachung nicht nur theoretisch möglich, sondern auch tatsächlich in großem Umfang statt findet, wurde bisher immer nur vermutet. Seit kurzem haben wir Gewissheit: Unternehmen wie staatliche Institutionen haben in den letzten Jahren Überwachungstechnik in Stellung gebracht, die bei weitem das übersteigt, was viele von uns für möglich hielten – und welches rechtlich zulässig wäre. Was genau hinter der Analogie zur Postkarte steckt und welche Möglichkeiten es gibt, unsere E-Mail-Korrespondenz vertraulich zu halten, möchten wir Ihnen im Folgenden erläutern.

Die unten stehende Skizze zeigt sehr vereinfacht den Weg, den eine E-Mail von A, unserem Mandanten, zu B in unserer Kanzlei nimmt. Die E-Mail verlässt das Netzwerk des Mandanten und durchquert das Internet, um das Netzwerk von bepartners zu erreichen. Auf ihrem Weg durch das Internet ist die unverschlüsselte E-Mail neugierigen Blicken schutzlos ausgeliefert. Ansatzpunkte für eine Überwachung gibt es einige, beispielsweise die an der Übertragung beteiligten Mailserver, aber auch die Netzwerkinfrastruktur auf einer tieferen Ebene. Doch dazu später.

Vertraulichkeit kann nur durch eine gute Verschlüsselung der Inhalte erreicht werden. Doch ist Verschlüsselung nicht gleich Verschlüsselung:

Im Falle der E-Mail ist zunächst zu differenzieren zwischen der Transportverschlüsselung und der Ende-zu-Ende-Verschlüsselung. Während die Transportverschlüsselung immer nur zwischen einzelnen am Übertragungsvorgang der E-Mail



beteiligten technischen Systemen erfolgt, ist eine Ende-zu-Ende-Verschlüsselung durchgängig: der Absender der E-Mail verschlüsselt die Inhalte für den Empfänger, und nur der Empfänger kann die Inhalte wieder entschlüsseln. Eine Ende-zu-Ende-Verschlüsselung würde demnach unsere Probleme lösen; über mögliche Schwachstellen der Transportverschlüsselung müsste man dann nicht mehr nachdenken.

Doch leider wird die Ende-zu-Ende-Verschlüsselung bisher nur selten eingesetzt. Dies hat natürlich seinen Grund. So ist bei einer solchen Verschlüsselung immer das Zusammenwirken von Absender und Empfänger erforderlich, beispielsweise der Austausch eines Schlüssels und das anschließende Einpflegen des Schlüssels durch die IT-Administration der Beteiligten. Die Einrichtung und Pflege bedeutet also zusätzlichen Aufwand und wurde in der Vergangenheit von vielen Unternehmen als nicht verhältnismäßig eingeschätzt. Wir meinen, die jüngsten Erkenntnisse geben Anlass zu einer Neubewertung dieser Situation. Doch lassen Sie uns betrachten, wo die Risiken liegen:

In den häufigen Fällen der fehlenden Ende-zu-Ende-Verschlüsselung kommt allenfalls eine Transportverschlüsselung zum Einsatz. Hier ist jedoch genau darauf zu achten, auf welchen Wegabschnitten die E-Mail verschlüsselt übertragen wird. Denn wie oben erwähnt, wird bei der Transportverschlüsselung nur jeweils zwischen den einzelnen technischen Systemen verschlüsselt – gerade nicht Ende-zu-Ende.

Sie kennen möglicherweise Verschlüsselungseinstellungen aus Ihrem E-Mail-Programm. Dort findet man häufig die Begriffe SSL/TLS bzw. STARTTLS. Dies meint Verfahren der Transportverschlüsselung; allerdings nur für den Streckenabschnitt von Ihrem E-Mail-Programm bis zu Ihrem verwendeten Mailserver – und nicht weiter! Die Einzelheiten der Transportverschlüsselung zwischen Mailservern an dieser Stelle auszubreiten, würde den Rahmen sprengen. Daher nur soviel: man kann sich als Anwender leider nicht darauf verlassen, dass bei der Übertragung von E-Mails zwischen den verschiedenen technischen Systemen, die eine E-Mail auf ihrem Weg zum Empfänger durch das Internet passiert, Verschlüsselung zum Einsatz kommt. Auch nicht dann, wenn der Absender die genannten Verschlüsselungsoptionen in seinem E-Mail-Programm aktiviert hat. Zurückzuführen ist dieser Umstand schlicht darauf, dass die dem Internet zugrunde liegende Technologie sehr alt ist und damals eine Nutzung wie sie heute erfolgt, nicht denkbar und nie beabsichtigt war. Entsprechend ist Verschlüsselung kein integraler Bestandteil der E-Mail-Infrastruktur, sondern nur durch spätere Ergänzungen hinzu gekommen. Aufgrund der Komplexität der Systeme war es jedoch nicht so einfach, Verschlüsselungstechnologien in die Abläufe zu integrieren ohne den Betrieb zu gefährden. In der Folge ist es technologisch bisher leider bei Stückwerk geblieben.

Im Ergebnis muss festgestellt werden, dass sich der Anwender leider nicht auf eine Transportverschlüsselung des gesamten Übertragungsweges seiner E-Mail verlassen kann. Er muss also damit rechnen, dass eine E-Mail, die nicht Ende-zu-Ende verschlüsselt wird, gänzlich unverschlüsselt durch das Internet zum Empfänger übertragen wird. Dadurch wird es möglich, Inhalte sogar durch Abhorchen der Internetleitungen irgendwo auf dem Übertragungsweg durch das Internet abzufangen, wie es beispielsweise durch den britischen Geheimdienst seit Jahren erfolgen soll.

Doch selbst wenn der Anwender das Glück hat, dass bei der Übertragung seiner E-Mail durchgehend Transportverschlüsselung zum Einsatz kommt; auf den an der Übertragung beteiligten Mailservern kann die E-Mail immernoch von allen Personen gelesen werden, die Zugriff auf diese Server haben. Da eine E-Mail nicht in jedem Fall direkt von Ihrem Mailserver an unseren Mailserver gesendet wird, sondern in bestimmten Konstellationen noch weitere Mailserver dazwischen geschaltet sein können, wird der Kreis der potentiellen Mitleser erhöht.

Ein vernünftiges Maß an Sicherheit bietet daher nur die Ende-zu-Ende-Verschlüsselung. Zum Einsatz kommen regelmäßig die Technologien S/MIME oder OpenPGP. Die Einrichtung und Pflege der entsprechenden Infrastruktur bedeutet sicherlich zusätzlichen Aufwand, abhängig von der konkret eingesetzten Lösung auf Seiten der Systemadministration oder auf Anwenderseite. Wir meinen jedoch, dass die jüngsten Erkenntnisse über das Ausmaß der Überwachung des Internets eine Neubewertung des Risikos der Kommunikation per E-Mail erforderlich macht. Mag man sich bisher auf den Standpunkt gestellt haben, dass eine Ende-zu-Ende-Verschlüsselung von E-Mails angesichts des zusätzlichen Aufwands, der administrativ getätigt werden muss, unverhältnismäßig ist, so spricht heute vieles dafür, der vertraulichen Kommunikation im Internet mehr Beachtung zukommen zu lassen.

Unsere Lösungen

Wir bieten Ihnen zwei Lösungen an, mit denen sich das Sicherheitsniveau unserer Kommunikation bzw. des Datenaustauschs mit einfachen Mitteln um ein Vielfaches steigern lässt: Einerseits die angesprochene E-Mail-Verschlüsselung Ende-zu-Ende, andererseits die Verwendung eines von uns betriebenen webbasierten Portals für den Datenaustausch, welches vor allem für die vertrauliche Übertragung von größeren Dateien in Betracht kommt.

E-Mail-Verschlüsselung

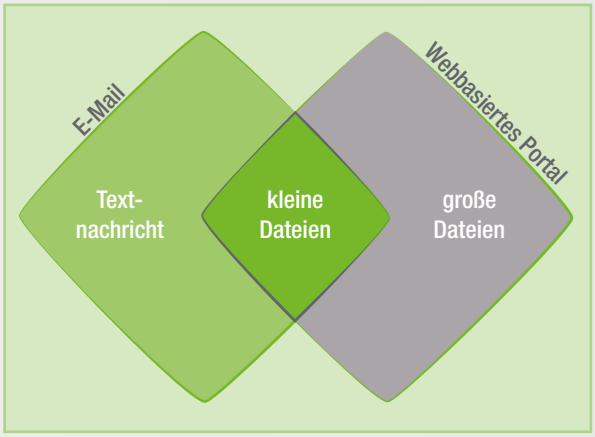
Bei der Ende-zu-Ende-Verschlüsselung von E-Mails kommen heute vor allem zwei technische Lösungen zu Einsatz: S/MIME und OpenPGP. Wir unterstützen beide Verfahren. Sprechen Sie uns an! Wir besprechen mit Ihnen dann gerne die Einzelheiten.

Webbasiertes Portal

Eine andere Variante der sicheren Datenübertragung stellt die Verwendung unseres Portals für den Datenaustausch dar. Gegenüber der E-Mail bestehen folgende Vorteile:

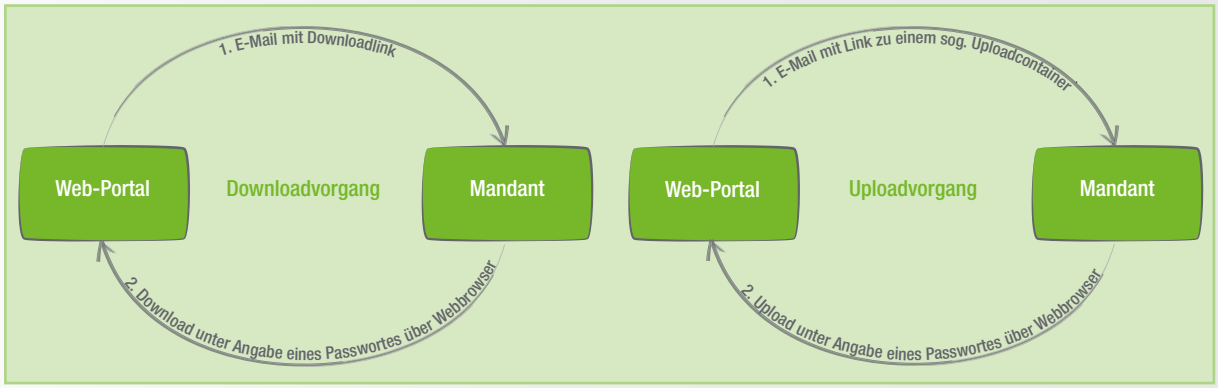
- Auf Ihrer Seite sind keine besonderen Softwareinstallationen erforderlich. Die Nutzung des webbasierten Portals für den Datenaustausch erfolgt ausschließlich über Ihren Webbrowser. Ihr Browser baut eine verschlüsselte Verbindung zu unserem Server auf. Dieser Server steht in unseren Kanzleiräumen und wird laufend überwacht.
- Im Gegensatz zur E-Mail ist es mit dem webbasierten Portal für den Datenaustauschauch möglich, große Datenmengen zu übertragen. Die Sicherheit der Datenübertragung ist damit nur ein Aspekt unseres webbasierten Portals für den Datenaustausch; es bietet auch Möglichkeiten, die mit dem Medium E-Mail nicht umsetzbar sind.

Nähere Informationen zur Nutzung unseres webbasierten Portals lassen wir Ihnen gerne zukommen.



Im optimalen Fall ergänzen sich die Instrumente der verschlüsselten E-Mail und des webbasierten Portals für den Datenaustausch. Während die E-Mail das bevorzugte Medium für kurze Textnachrichten und kleine Dateien ist, ermöglicht das webbasierte Portal für den Datenaustausch die verschlüsselte Übertragung auch großer Datenmengen.

Wir hoffen, die oben stehenden Ausführungen waren für Sie interessant. Wenn Sie Ihre elektronische Kommunikation mit uns sicherer gestalten möchten, sprechen Sie uns bitte an.



bei Rückfragen stehen wir Ihnen gerne zur Verfügung.

Dr. Carsten Bödecker
Partner . Steuerberater . Rechtsanwalt

Tel. +49 (0) 211 946847-51
Fax +49 (0) 211 946847-01

carsten.boedecker@bepartners.pro

Carsten Ernst
Partner . Steuerberater

Tel. +49 (0) 211 946847-52
Fax +49 (0) 211 946847-01

carsten.ernst@bepartners.pro

Harald Kuhn
Partner . Rechtsanwalt

Tel. +49 (0) 211 946847-54
Fax +49 (0) 211 946847-01

harald.kuhn@bepartners.pro

Hendrik Sünkler
IT-Strategie . Technology Evangelist

Tel. +49 (0) 211 946847-61
Fax +49 (0) 211 946847-01

hendrik.suenkler@bepartners.pro