

Sicherer Dokumentenaustausch via E-Mail

Tauschen Sie sensible Informationen wie persönliche Zugangsdaten und sensible Unternehmensdaten nur verschlüsselt aus! Jede unverschlüsselte E-Mail ist wie eine Postkarte. Jeder der sie zu sehen bekommt, kann sie sofort lesen. So wandern schützenswerte Informationen vom „Postkasten“ über Zwischenstationen im Internet bis hin zum „Briefkasten“ des Empfängers heute leider immer noch viel zu häufig unverschlüsselt! Damit sind Ihre Daten, für viele die Interesse an Ihren Informationen haben, an vielen Stellen abgreifbar! Darüber hinaus kleben E-Mails nach dem Empfang sicherlich nicht wie Postkarten auf dem Kühlschrank, doch sind sie meist unverschlüsselt auf der Festplatte hinterlegt. Ist Ihr Rechner kurze Zeit unbeaufsichtigt oder wurde via E-Mailversand ein Trojaner installiert, kann ein Spion schnell an Ihre sensiblen Informationen gelangen.



Damit Sie nicht Gefahr laufen, dass Ihre persönlichen Daten oder sensible Unternehmensinformationen in die falschen Hände gelangen, sollten Sie diese ausschließlich in einem „geschlossenen Briefumschlag“ versenden. Wird die E-Mail verschlüsselt können nur Empfänger und Absender diese mit ihrem Passwort entschlüsseln. Eine E-Mail sollte vor allem dann verschlüsselt werden, wenn vertrauliche Informationen nur für den Absender und Empfänger dieser E-Mail bestimmt sind. Sind die technischen Voraussetzungen für die E-Mail-Verschlüsselung einmal geschaffen, können Sie Ihre E-Mails zugleich auch digital signieren. Mit Hilfe Ihrer E-Mail Signatur kann Ihr gegenüber erkennen, dass Ihre E-Mail nicht von Dritten manipuliert worden ist und dass auch wirklich Sie diese E-Mail verfasst haben! Durchgesetzt hat sich vor allem die so genannte PKI-basierte E-Mail-Verschlüsselung und -Signatur.

PKI steht für „Public Key Infrastructure“. Bei der PKI-basierten Anwendungsform kommt meist einer von zwei verschiedenen Standards zum Einsatz. Dies ist zum einen S/MIME, der vermehrt in größeren Unternehmen verwendet wird und zum anderen OpenPGP, der schnell und unabhängig ohne Unternehmensserver auf dem Computer des Anwenders betrieben werden kann. Damit Sie sich möglichst schnell mit dem Thema vertraut machen können, wird OpenPGP als Grundlage in diesem IT-Sicherheitstipp verwendet.

Die Public Key Infrastructure hat den großen Vorteil, dass bei einem verschlüsselten E-Mailaustausch nicht jedes Mal im Vorfeld ein geheimes Passwort für die Ver- und Entschlüsselung ausgetauscht werden muss. Sowohl Absender als auch Empfänger, die am Austausch verschlüsselter E-Mails beteiligt sind, verfügen über jeweils zwei Schlüssel – dem so genannten Schlüsselpaar. Dies setzt sich aus einem privaten und öffentlichen Schlüssel zusammen und wird in einer Datei gespeichert. Der öffentliche Schlüssel des Empfängers ist dem Absender bekannt und kann wie eine Telefonnummer über Verzeichnisdienste im Internet schnell und einfach gefunden werden. Der private Schlüssel hingegen ist ausschließlich im Besitz des Absenders und in Analogie zu einer EC-Karte mit PIN, mit einem Passwort geschützt. Mit dem öffentlichen Schlüssel seines Empfängers kann der Absender seine E-Mail verschlüsseln. Nur mit dem privaten Schlüssel des Empfängers kann nun die Nachricht entschlüsselt werden. Obwohl die Verschlüsselungsmethode als so sicher gilt, dass auch staatliche Organe wie Geheimdienste PGP-verschlüsselte E-Mails nicht entschlüsseln können, sollten Sie einige Tipps bei der verschlüsselten E-Mailkommunikation beachten!

► **Geben Sie Ihren privaten Schlüssel niemals preis!**

Wie Sie nun erfahren haben, können für Sie verschlüsselte E-Mails mithilfe Ihres privaten Schlüssels entschlüsselt werden. Dieser liegt Ihnen in einer Datei vor, die mit einem Passwort Ihrer Wahl geschützt ist. Gelangt nun Ihr privater Schlüssel und Ihr Passwort in falsche Hände, können alle Ihre E-Mails entschlüsselt und damit vertrauliche Informationen eingesehen werden. Darüber hinaus kann der Dieb E-Mails scheinbar in Ihrem Namen verfassen und Sie in Ihrem Namen elektronisch signieren! Gehen Sie daher besonders behutsam mit Ihrem privaten Schlüssel und Passwort um! Geben Sie Ihren Schlüssel keinesfalls weiter und speichern Sie diesen an sicherer Stelle.

► **Verwahren Sie Ihren privaten Schlüssel an einem sicheren Ort!**

Speichern Sie Ihren privaten Schlüssel nicht auf einem Rechner, auf den Dritte Zugang haben. Verwenden Sie diesen nur auf Ihrem eignen Rechner. Andernfalls laufen Sie Gefahr, dass Dateien wie Ihr Schlüssel kopiert und Eingaben wie Passwörter unbemerkt protokolliert werden. Achten Sie darauf, dass Sie Ihren privaten Schlüssel bei Nichtgebrauch vor fremdem Zugriff schützen! Gerade als Neuling sollten Sie darauf achten, dass Sie nicht versehentlich Ihr gesamtes Schlüsselpaar, inklusive privaten Schlüssel, als vermeintlich öffentlichen Schlüssel weitergeben!

► **Erstellen Sie eine Sicherungskopie Ihres privaten Schlüssels auf externen Medien!**

Besitzen Sie keine Datensicherung, so verlieren Sie bei einem Totalausfall Ihres Systems meist auch Ihren privaten Schlüssel. Erstellen Sie deshalb regelmäßig eine Datensicherung Ihrer Daten auf einem externen Medium. Bewahren Sie die Datensicherungen an einem sicheren Ort auf! Empfehlenswert ist es, die Daten nicht am selben Ort wie die Originaldaten aufzubewahren. Bei einem Brand oder Diebstahl wären neben Ihren Originaldaten dann auch Ihre Datensicherungen in großer Gefahr! Achten Sie bei Ihren Datensicherungen darauf, dass Sie auch Ihren privaten Schlüssel sichern!

► **Gelangt Ihr privater Schlüssel in falsche Hände, erklären Sie ihn für ungültig!**

Für den Fall, dass Sie Ihren privaten Schlüssel verlieren oder überzeugt sind, dass dieser kopiert und gestohlen wurde, erklären Sie Ihr Schlüsselpaar sofort für ungültig! Da Ihr privater und öffentlicher Schlüssel aufeinander abgestimmt sind, müssen Sie bei einem Verlust ein neues Schlüsselpaar erstellen. Damit ihr bisheriges Schlüsselpaar nicht von Dritten in Ihrem Namen verwendet werden kann, sollten Sie dieses umgehend mit einem so genannten „revoke-Zertifikat“, das Sie bei jeder Schlüsselpaarerstellung erhalten, für ungültig erklären. Dieser Vermerk wird direkt in die Verzeichnisdienste eingetragen und Ihr öffentlicher Schlüssel aus diesen gelöscht.

► **Überprüfen Sie zu Beginn den öffentlichen Schlüssel Ihres Empfängers!**

Grundsätzlich kann jeder in Ihrem Namen eine E-Mailadresse erstellen. Meist werden bei E-Maildiensten zwar die persönlichen Daten verlangt eine Verifikation dieser Daten findet jedoch nur selten statt.

Auch bei der Erzeugung eines OpenPGP-Schlüsselpaars, das sich nun auf Ihre scheinbar neue E-Mailadresse bezieht, ist kein Identifikationsnachweis erforderlich. Damit kann sich jemand als Sie ausgeben. Möchte Ihnen nun ein Geschäftspartner vertrauliche Informationen übermitteln, so schaut er im Verzeichnisdienst nach Ihrer E-Mailadresse und Ihrem öffentlichen Schlüssel nach. Sofern Sie nicht selber dort einen öffentlichen Schlüssel hinterlegt haben oder Ihrem Geschäftspartner Ihre E-Mailadresse nicht bekannt ist, wählt er unter Umständen einen falschen öffentlichen Schlüssel aus – den des Spions! Ihr Geschäftspartner sendet daraufhin vertrauliche Informationen im guten Glauben an Sie. Doch die Daten gelangen in die Hände des Spions. Um sich davor zu schützen, müssen Sie vor dem Versenden Ihrer Daten den für die Verschlüsselung notwendigen öffentlichen Schlüssel Ihres Empfängers auf Echtheit überprüfen! Dazu dient das Web of Trust. Eine Gemeinschaft von Vertrauensbeziehungen. So können Personen untereinander öffentliche Schlüssel von Bekannten mit ihrem privaten Schlüssel als gültig einstufen und diesen unterzeichnen. Hat den für die verschlüsselte Kommunikation gesuchten Schlüssel auch eine Person unterzeichnet der Sie vertrauen, handelt es sich offenkundig um den richtigen Schlüssel, den Sie suchen! Das Netzwerk ist transparent und für jeden einsehbar und eine der Grundideen von OpenPGP. Um Ihren Partnern die Suche und Verifikation Ihres öffentlichen Schlüssels zu erleichtern, können Sie auch über Ihre Webseite auf Ihren öffentlichen Schlüssel verweisen. Beispiel: <https://www.internet-sicherheit.de/spooren/>

► **Wählen Sie starke Passwörter!**

Passwörter werden nach Ihrer Stärke gemessen. Je länger ein Passwort ist und umso mehr verschiedene Zeichen es enthält, umso stärker der Schutz. Stellen Sie sich dazu einfach einen Aktenkoffer vor. Je mehr Kombinationsmöglichkeiten das Zahlenschloss besitzt, umso geringer ist die Wahrscheinlichkeit, dass ein Angreifer diesen öffnen kann. Zudem sollten Sie bei Passwörtern beachten, dass sie sinnfrei zusammengesetzt werden und nicht wie häufig, aus dem Namen oder Geburtsdatum des Partners bestehen – die sind von einem vertrauten Angreifer schnell erraten. Verwenden Sie zum Schutz sensibler Daten stets ein starkes Passwort. Passwörter sollten aus mindestens zehn Zeichen und Ziffern bestehen, Sonderzeichen, sowie Groß- und Kleinschreibung enthalten und nicht aus existierenden Wörtern zusammengesetzt sein.

Werden diese Kriterien beachtet, spricht man von einem starken Passwort. Ein Beispiel für ein starkes Passwort ist „Aj1.u3.SiMsiF!“. Um sich ein starkes Passwort zu merken, prägen Sie sich im Vorfeld einen Satz gut ein. Mit Hilfe dessen können Sie sich jederzeit ein starkes Passwort erstellen. Zum Beispiel: „An jedem 1. und 3. Samstag im Monat spiele ich Fußball!“. Für das Passwort verwenden Sie nun einfach die Anfangsbuchstaben und Satzzeichen eines jeden Wortes. Daraus ergibt sich: „Aj1.u3.SiMsiF!“. Geben Sie Ihr Passwort oder Ihren dazugehörigen Merksatz niemals Dritten preis! Immer wieder tauchen Datenskandale auf, in denen bekannt wird, dass Tausende von Benutzerdaten gestohlen worden und nun im Umlauf sind. Verwenden Sie deshalb nie ein Passwort doppelt. Andernfalls laufen Sie Gefahr, dass Ihre gestohlenen Benutzerdaten für weitere Dienste, wie Online-Banking, verwendet werden können.

► **Achten Sie auf den notwendigen Basisschutz!**

Trojaner können Ihren privaten Schlüssel ausspionieren.

Schadprogramme wie Trojaner stellen ein großes Sicherheitsrisiko dar. Verfügt Ihr Rechner nicht über ausreichende Schutzprogramme, ist es schnell passiert. Sie klicken ein scheinbar nützliches Programm an, welches Ihnen via E-Mail zugesandt worden ist. Doch in dem nützlichen Programmcode verbirgt sich Schadcode. Sobald Sie das Programm öffnen, wird dieser ausgeführt und beispielsweise ein Trojaner auf Ihrem Rechner installiert. So genannte Keylogger speichern alle von Ihnen gemachten Eingaben mit, so zum Beispiel auch Ihr Passwort, um den privaten Schlüssel zu benutzen. Liegt Ihr privater Schlüssel auf Ihrer Festplatte, können Kriminelle über den Trojaner Ihren privaten Schlüssel kopieren und daraufhin Ihre vertraulichen Informationen entschlüsseln. Um sich vor Schadprogrammen angemessen zu schützen, ist es deshalb stets erforderlich, dass Sie ein aktuelles Antivirenprogramm verwenden. Achten Sie darauf, dass Sicherheitsupdates regelmäßig durchgeführt werden und sich alle Programme immer auf dem neuesten Stand befinden. Verwenden Sie eine aktuelle Personal-Firewall für Ihren Computer. Betriebssysteme wie Windows XP, Vista und 7 haben diese bereits von Haus aus integriert. Nicht nur das Virenschutzprogramm, sondern auch das Betriebssystem sowie alle installierten Anwendungen sollten beim Erscheinen von Sicherheitsupdates umgehend aktualisiert werden. Updates können vom Betriebs-

system und den meisten Programmen automatisiert durchgeführt werden. Überprüfen Sie dazu die Sicherheitseinstellungen bei Ihrem Betriebssystem.

Autoren:

*Dipl.-Inform.(FH) Sebastian Spooren, Prof. Dr. Norbert Pohlmann
Institut für Internet-Sicherheit – if(is), Fachhochschule Gelsenkirchen*

Weiterführende Informationen:

<http://www.internet-sicherheit.de>

<http://www.branchenbuch-it-sicherheit.de>

<http://www.gpg4win.de/>

Das Institut für Internet-Sicherheit – if(is)

Das Institut für Internet-Sicherheit ist eine fachbereichsübergreifende wissenschaftliche Einrichtung der Fachhochschule Gelsenkirchen. Es forscht und entwickelt auf Basis innovativer Konzepte im Bereich der Internet-Sicherheit. 2005 gegründet, hat es sich unter der Leitung von Prof. Dr. Norbert Pohlmann und in enger Zusammenarbeit mit der Wirtschaft innerhalb kurzer Zeit einen Ruf als eine der führenden deutschen Forschungsinstitutionen der IT-Sicherheit gemacht. Weitere Informationen finden Sie unter: <http://www.internet-sicherheit.de>

Sichere E-Geschäftsprozesse in KMU und Handwerk

Der IT-Sicherheitstipp wurde im Rahmen des Verbundprojekts „Sichere E-Geschäftsprozesse in KMU und Handwerk“ des Netzwerks Elektronischer Geschäftsverkehr (NEG) erstellt. Das Verbundprojekt wird vom Bundesministerium für Wirtschaft und Technologie (BMWi) unterstützt und soll helfen, in kleinen und mittleren Unternehmen mit verträglichem Aufwand die Sicherheitskultur zu verbessern. Hier werden insbesondere kleine und mittelständische Unternehmen sowie das Handwerk zu wichtigen Aspekten der Informationssicherheit sensibilisiert und praxisnah informiert. Alle Details finden Sie unter: <http://www.ec-net.de/sicherheit> sowie unter: http://www.ecc-handel.de/sichere_e-geschaeftsprozesse_in_kmu_und_handwerk.php

Bildquelle: Spectral-Design – Fotolia.com