

Leben

Heute:
Computer
& Web

E-Mails mit eigenem Schlüssel

Von: marcus.schwarze@rhein-zeitung.net**An:** die Leser der Rhein-Zeitung**Betreff:** Der Traum vom abhörsicheren Kommunizieren ist schwieriger zu erfüllen, als mancher denkt

E-Mails zu verschlüsseln, würde dabei helfen, sich gegen Spionage abzusichern. Nur Absender und Empfänger können dann den Text lesen oder enthaltene Dateien sichtbar machen. Das ist allerdings in der Praxis schwieriger als gedacht. Die Verschlüsselung ist in der Theorie ganz einfach. Stark vereinfacht dargestellt, funktioniert sie so: Man nehme einen Text ABC, verschiebe ihn um x Zeichen im Alphabet und dann noch einmal um y Zeichen. Wenn x = 2, erhält man die Zeichenfolge CDE. Und wenn y = 3, erhält man FGH.

Warum macht man das zweimal? Weil es jeweils einen privaten und einen öffentlichen Schlüssel braucht, um das System besser zu verschleiern. Meinen privaten Schlüssel x kenne nur ich; meinen öffentlichen Schlüssel y lege ich für jedermann zum Abrufen auf einem Schlüsselservers ab. Will mir nun ein Fremder eine E-Mail schicken, benötigt er zunächst meinen öffentlichen Schlüssel und chiffriert seine E-Mail an mich damit. Aus seiner E-Mail ABC wird dann DEF. Erst, wenn ich meinen privaten Schlüssel hinzufüge, wird daraus FGH. Und da nur ich selbst über beide Schlüssel verfüge, kann ich aus FGH den Ursprungstext ABC zurückberechnen.

In der Praxis ist das Verfahren noch wesentlich komplexer und reicht weit über das Verschieben von Buchstaben im Alphabet hinaus. Die beiden Schlüssel werden auf einer gemeinsamen mathematischen Basis generiert und machen es so möglich, dass man einen Text im ersten Gang mit seinem priva-

ten Schlüssel und im zweiten Gang mit dem öffentlichen Schlüssel des Gegenübers chiffriert. Der kann dann umgekehrt mit seinem privaten Schlüssel und dem öffentlichen

Schlüssel des Absenders das Ganze lesbar machen.

Im jeweiligen Programm ist das, sofern einmal richtig installiert, nur ein Klick – der dann aber zusätzlich durch die Eingabe einer sogenannten Passphrase kompliziert wird. Dabei handelt es sich um ein Kennwort, das man beim Einrichten der Verschlüsselung festgelegt hat. Einen besonders einfachen Weg zum Anlegen einer neuen E-Mail-Adresse, die standardmäßig Verschlüsselung nutzt, bietet der Dienst private.ki aus Mainz. Er

funktioniert unter der gleichnamigen Internetadresse direkt im Browser.

Um Verschlüsselung zu nutzen, wird es nötig, dass alle Teilnehmer des E-Mail-Verkehrs solche Schlüsselpaare generiert haben. Und da liegt der Hase im Pfeffer. Nicht jedem ist die Handhabung der üblichen Programme Pretty Good Privacy (PGP) oder OpenPGP geläufig. Man muss auf Dauer jeden öffentlichen Schlüssel seines Gegenübers mühsam in sein eigenes Adressbuch einpflegen. Und jeder E-Mail-Adressat, mit dem man verschlüsselt kommunizieren möchte, muss das Gleiche tun. In der Firmenwelt hat sich zudem ein etwas anderes Verschlüsselungsverfahren namens S/Mime etabliert, bei dem öffentliche Zertifikate von Zertifizierungsstellen ausgestellt werden. Da kann man dann nicht einfach seinen öffentli-

chen Schlüssel irgendwo hochladen, sondern muss sich je nach Qualität des gewünschten Zertifikats mit dem Personalauswahl persönlich authentifizieren. Außerdem arbeiten die gängigen E-Mail-Programme nicht ad hoc mit PGP und Co. zusammen. Je nach Betriebssystem und E-Mail-Programm sind unterschiedliche Installations-schritte nötig. Eine einfache, wenn auch alte Anleitung gibt es unter <http://ku-rz.de/pgphilfe>

+ Wenn Sie dem Autor eine verschlüsselte Nachricht schicken möchten: Seinen öffentlichen Schlüssel für die E-Mail-Adresse marcus.schwarze@rhein-zeitung.net finden Sie unter <http://ku-rz.de/keymasc>

➔ Wer Verschlüsselung einmal unter einer neuen E-Mail-Adresse ausprobieren möchte, kann dies unter www.private.ki kostenlos tun.



Serie

**Schritt für Schritt ins Internet**

Unsere Serie für Einsteiger

Teil 28: Einstieg bei YouTube
Teil 29: Gespeicherte Bilder
Teil 30: Instagram
Teil 31: Verschlüsselte E-Mail

Wie sicher ist Verschlüsselung?

Seit den Enthüllungen des NSA-Mitarbeiters Edward Snowden muss jedermann im Internet befürchten, dass seine E-Mails oder sein Surfverhalten von Fremden ausspioniert werden können. „Können“ heißt dabei: Milliardenfach liegen E-Mails und Dateien nur brach, und bestimmte Dienste haben die Möglichkeit, jemanden auszuspionieren. Die genauen Fähigkeiten der Geheimdienste sind unbekannt, jedoch deuten viele Hinweise darauf hin, dass einfache E-Mails nachge-

lesen werden können. Mit der Verschlüsselung macht man es den Spionen schwerer. Einfache Verschlüsselungsmechanismen kann heute ein Hacker aushebeln. Die Frage ist, wie viel Energie ein Spion darauf verwendet. Die komplexen Verfahren zur Verschlüsselung lassen sich häufig durch ganz andersartige Schnüffelei knacken, etwa durch eine Kamera, die von gegenüber durchs Fenster auf den Monitor gerichtet wird, oder durch eine Trojanersoftware, die per ver-

trauenswürdig erscheinender E-Mail auf den Rechner des Opfers geschleust wird. Die protokolliert jede Tastatureingabe oder erstellt auf die Schnelle Bildschirmfotos, die übers Internet versandt werden. 100-prozentige Sicherheit gibt es bei der Internetkommunikation nicht. Mit genügend Aufwand ist alles knackbar. Aber es ist ein Unterschied, ob fürs Ausspionieren einer E-Mail eine Sekunde oder die Rechenkraft von fünf Servern für zehn Stunden benötigt wird. Dem dient die Ver-

schlüsselung. Wer sagt, er habe nichts zu verbergen, sollte stets bedenken, dass es Leute gibt, die zu Recht etwas zu verbergen haben. Denen hilft man durch eigene Verschlüsselung, denn entschlüsseln dürfen per Gesetz nur Befugte. Die NSA und jeder Hacker ist nach deutschem Recht aber nicht dazu befugt, Ihre verschlüsselte E-Mail an den Autor dieses Textes zu entschlüsseln, und wollten Sie nur auf den fehlenden Punkt am Ende dieses Satzes hinweisen *msc*

Experte: Kostenpflichtiger E-Mail-Dienst lohnt sich nicht

Von: stefan.hantzschmann@rhein-zeitung.net**An:** die Leser der Rhein-Zeitung**Betreff:** Uwe Arndt hat die Anfänge der E-Mail in Koblenz erlebt

Gerade ein paar Jahre nachdem die erste E-Mail in Deutschland empfangen wurde, arbeitete Uwe Arndt an dem ersten E-Mail-System für die Universität Koblenz. Im Interview erklärt der Leiter des Rechenzentrums der Uni Koblenz unserer Zeitung, welche Probleme E-Mails verursachen und wie man den Überblick behält.

Hallo Herr Arndt! Können Sie sich noch an Ihre erste E-Mail erinnern? Nein, nicht direkt. Aber ich kann mich noch gut an das erste E-Mail-System der Uni Koblenz erinnern. Das war vor etwa 28 Jahren, noch bevor das Internet an den meisten Universitäten überhaupt verfügbar

war. Es konnte damals Stunden dauern, bis eine Mail ihren Empfänger erreichte. Heute gehören E-Mails schon fast zur Echtzeit-Kommunikation. Allein am Koblenzer Campus haben wir 14 000 Nutzer, die pro Monat etwa sechs Millionen Nachrichten versenden und empfangen.

Heute gibt es unzählige E-Mail-Anbieter und verschiedene Protokolle. Welches Protokoll ist für einen Privatanwender das richtige? Die großen, wichtigen Protokolle sind POP3 und Imap, wenn Sie einen E-Mail-Klienten verwenden. Beide Protokolle sind gut, empfehlen würde ich aber Imap. Einige

Anbieter verlangen dafür einen Aufpreis; es gibt aber auch kostenlose Angebote. Der Vorteil von Imap ist, dass man die Nachrichten auf dem Server lassen kann und somit auch von fremden Rechnern Zugriff auf empfangene und gesendete E-Mails hat. Auch die Synchronisierung funktioniert besser.

Lohnt sich für Durchschnittsanwender ein kostenpflichtiger E-Mail-Dienst?

Ich würde sagen: nein. Die kostenlosen Anbieter verdienen ihr Geld dadurch, Ihnen ab und zu eine Werbe-Mail zu schicken und Werbung auf der Login-Seite zu platzieren. Andere, wie Google, scannen Ihre E-Mails, um Ihnen dann passende Werbung anzeigen zu können. Wenn wir E-Mails versenden – wie bei jeder Aktivität im Internet –, hinterlassen wir Spuren, es sei denn, das geschieht innerhalb eines geschlossenen Netzwerkes – zum Beispiel einer Uni oder Firma.

Hat die Kommunikation in sozialen Netzwerken wie Facebook oder mithilfe von Diensten wie WhatsApp das Ende der E-Mail-Ära eingeleitet?

Das glaube ich nicht. WhatsApp und Facebook haben nicht den „antiken“ Touch von E-Mails. Aber die Nachrichten lassen sich kaum ordnen und archivieren. Zudem wirkt eine E-Mail-Korrespondenz seriöser. Die Kommunikation zwischen Firmen läuft hauptsächlich per E-Mail ab.

Wenn ich mein Postfach anschau, habe ich nicht den Eindruck, dass sich E-Mails besonders leicht ordnen lassen ...

(lacht) Eine volle Inbox ist der Tod jeder Kommunikation. Ganz einfach: Sie müssen Ihre Mails regelmäßig abarbeiten und sortieren. Im Prinzip gibt es ja nur drei Möglichkeiten: löschen, im Eingang belassen, archivieren. Ich bin davon überzeugt, dass zu viele Filtereinstellungen, die Ihre E-Mails auto-

matisch in Ordner einsortieren, das Chaos nur verstärken.

Das Platzproblem im Postfach rührt auch daher, dass immer größere E-Mails verschickt werden. Was kann ich dagegen tun?

Das stimmt. Bei uns im Rechenzentrum passieren ungefähr ein Terabyte, also 1000 Gigabyte, E-Mails unsere Server – pro Monat. Einige Anbieter setzen die Datengrenze bei 10 oder 20 Megabyte pro Mail. Wenn Sie Urlaubsfotos an Freunde schicken wollen, können Sie die Fotos bei einem Cloud-Dienst im Internet ablegen und Ihren Freunden nur den Link per E-Mail senden.

Das Gespräch führte
Stefan Hantzschmann

➔ Ein Gespräch mit dem Mathematiker René Pickhardt über die Zukunft der E-Mail lesen Sie auch im Internet unter der Adresse www.ku-rz.de/pickhardt

Kolumne

Marcus Schwarze
 über zu speichernde E-Mails



Ausgedruckt hilft es auch nichts

Die ersten Worte eines Kindes notiert man sich ja gern – sei es im Fotoalbum, auf einer Postkarte an die Verwandtschaft oder vielleicht auch bei Facebook. Die erste E-Mail vom Nachwuchs allerdings ist schnell verschüttet. Inmitten von Zehntausenden E-Mails geht so ein kleines Dokument der persönlichen Zeitgeschichte schnell verloren. Mein Sohn hat mir im zarten Alter vor ein paar Jahren aus einem Kinderhort seine erste E-Mail zugesandt, wunderbar angeleitet von einer Hortbetreuerin, die Wert auf eine ordentliche Anrede und eine persönliche Schlussformel legte. In zwei Sätzen ging es um „Spaghetti“ und „lecker“, einen sehr persönlichen Satz und für mich nach gefühlt 100-facher Lektüre um die entscheidende Frage: Wie bewahrt man so etwas auf?

Inmitten von 150 000 E-Mails, die ich im Berufs- und Privatleben nie weggeschmissen habe, geht so etwas unter. Also brachte ein Drucker die E-Mail zu Papier. Der Ausdruck hing eine Weile an der Wand und einen Arbeitgeberwechsel später im Büro. Als mal wieder Aufräumen angesagt war, landete das vergilbte Dokument auf einem Stapel, der mir nun wieder in die Hände fiel. Wohin jetzt damit?

Ich scannte also das Papierdokument ein, machte eine Bilddatei der einst ausgedruckten E-Mail, die nun im Familienverzeichnis der Fotos auf der Festplatte landete. Aber ach je: Dort residiert die Datei nun inmitten von 11 000 halbwegs oder gar nicht verschlagworteten Fotos, rudimentär benannten stundenlangen Videos und lediglich nach Datum sortierten Sounddateien erster Gitarren- und Flötenversuche der Kinder.

Wiedergefunden habe ich in einer halbstündigen Recherche weder die E-Mail noch das digitale Bild davon, und vor dem 24 Zentimeter hohen Papierstapel „2011“ im Büro habe ich gehörigen Respekt. Irgendwo dürften die Dateien sein, sogar zweifach gesichert durch ein tägliches Back-up auf einer zweiten Festplatte und durch ein zusätzliches auf einem Server. Aber bei nächster Gelegenheit, das weiß ich, da gibt's Spaghetti, und zwar leckere.

+ Machen Sie mit bei meinem kleinen Experiment: Senden Sie mir eine aufbewahrenswerte, besonders bemerkenswerte E-Mail. Die ersten 100 Einsendungen sammeln und speichern wir in einer Fotostrecke auf Rhein-Zeitung.de – vielleicht nicht für alle Ewigkeit, aber bestimmt eine kleine Ewigkeit lang und machen sie damit schnell auffindbar. Schicken Sie die E-Mail im Wortlaut oder als Screenshot an die Mailadresse marcus.schwarze@rhein-zeitung.net mit dem Betreff „E-Mail-Archiv“. Vollständige Namen werden wir schwärzen. Absender und Empfänger müssen mit der anonymisierten Veröffentlichung einverstanden sein.

Kompakt

Schwupps – und man zahlt fürs Postfach

E-Mails. Augen auf beim Einloggen ins E-Mail-Postfach: Manche Anbieter versuchen dabei, Nutzern des Gratis-Dienstes die kostenpflichtige Variante unterzujubeln. Die Verbraucherzentrale Nordrhein-Westfalen rät, bei unerwarteten Einblendungen und Angeboten auf dem Weg zum Postfach die Beschriftung der Buttons und Links sorgfältig zu lesen. Denn: Ein vorschneller Klick könnte zum Kauf führen. Wer aus Versehen daraufgeklickt hat, sollte sofort den Kauf kündigen. Verbraucher haben ein 14-tägiges Widerrufsrecht.