Sicherer E-MailVersand dank Verschlüsselung

Teil 1
Versionen: Outlook 2013, 2010, 2007, 2003 und 2002/XP

Würden Sie Ihren letzten Kontoauszug oder Ihre letzte Gehaltsabrechnung auf einer Postkarte verschicken? Vermutlich nicht. Und warum verschicken Sie Ihre E-Mails dann immer noch unverschlüsselt? Unverschlüsselte E-Mails sind genauso öffentlich wie Postkarten und können auf ihrem Weg durchs Internet von jedem gelesen werden. Wir empfehlen: Nutzen Sie moderne Verschlüsselungstechniken, um Ihre E-Mails abzusichern. Das ist leichter als Sie denken, denn die Techniken sind in Outlook schon eingebaut. In diesem dreiteiligen Tipp machen wir Sie mit den Schutzmechanismen vertraut.

Die E-Mail-Verschlüsselung fristete lange Zeit ein Schattendasein. Erst seit den Enthüllungen von Edward Snowden ist das Thema plötzlich topaktuell, denn kaum jemand will, dass die NSA oder andere Geheimdienste alles mitlesen, was man so per E-Mail verschickt. Aber wie schützen Sie sich vor der Überwachung?

Die desillusionierende Antwort: Im Prinzip können Sie sich gar nicht schützen, da die NSA fast überall Hintertüren eingebaut hat. In vielen Standardprogrammen, ja sogar in den gängigen Betriebssystemen gibt es Lücken, die zumindest theoretisch zum Ausspionieren benutzt werden können. Doch es gibt auch eine gute Nachricht: Es ist unwahrscheinlich, dass die NSA tatsächlich jeden einzelnen Computer belauscht. Im Zentrum der Überwachung stehen die Serverknoten im Internet, von denen jeglicher Datenverkehr abgegriffen wird. So kommen zwar auch Ihre E-Mails in die Fänge der Geheimdienste. Aber wenn Sie diese verschlüsseln, machen Sie es den Abhörspezialisten zumindest etwas schwerer, Ihren persönlichen Nachrichtenaustausch zu verfolgen.

Outlook unterstützt Sie sogar ab Werk bei der E- Mail-Verschlüsselung. Sie müssen also nicht einmal zusätzliche Programme installieren. Outlook setzt dabei auf den "S/MIME-Standard" (Secure Multipurpose Internet Mail Extensions), mit dem Sie E-Mails sowohl verschlüsseln als auch mit einer digitalen Signatur versehen können, die garantiert, dass die Nachricht von Ihnen stammt.

Sollten Ihnen Funktionen, die in ein Microsoft- Produkt eingebaut sind, zu unsicher erscheinen, können Sie Ihre E-Mails auch mit der freien Kryptografiesoftware GnuPG (GNU Privacy Guard) verschlüsseln. Die Installation und Bedienung erfordert allerdings größeren Aufwand.

Genau da liegt das Hauptproblem, warum E-Mail- Verschlüsselung noch nicht weiter verbreitet ist. Selbst die in Outlook eingebauten S/MIME-Funktionen erfordern ein paar zusätzliche Konfigurationsschritte. Und nicht nur Sie selbst müssen tätig werden. Auch alle Personen, mit denen Sie E-Mails austauschen, müssen das Verschlüsselungsverfahren einsetzen. Damit Sie besser verstehen, warum diese Schritte nötig sind, wollen wir Ihnen zuerst das Prinzip vorstellen, auf dem sowohl S/MIME als auch GnuPG aufbauen.

Um eine E-Mail zu verschlüsseln, brauchen Sie einen Code, mit dem sich die E-Mail später wieder entschlüsseln lässt. Da könnte man natürlich ein einfaches Passwort verwenden, das sowohl dem Sender als auch dem Empfänger der E-Mail bekannt ist. Das Problem: Wie tauschen Sie das Passwort aus? Ein Versand via Internet scheidet aus, weil das Passwort während der Übertragung mitgelesen werden könnte. Eine Alternative wäre der Austausch per Briefpost oder Telefon. Das wäre zwar etwas sicherer, aber viel zu kompliziert, wenn Sie auf diese Weise täglich unzählige Mails verschlüsseln wollten.

So kommen asymmetrische Verschlüsselungsverfahren ins Spiel. Dabei handelt es sich um Verfahren, die nicht nur auf einem einzigen Schlüssel/Passwort basieren sondern auf einem Schlüsselpaar. Es gibt einen "privaten Schlüssel", der der höchsten Geheimhaltungsstufe unterliegen sollte, und einen "öffentlichen Schlüssel", der beliebig an Empfänger verteilt oder sogar auf einem Verzeichnisserver im Internet veröffentlicht werden kann.

Das Ganze funktioniert nach folgendem Prinzip: Wenn Sie eine sichere E-Mail verschicken wollen, erstellen Sie mit dem öffentlichen Schlüssel des Empfängers eine codierte Nachricht. Decodiert werden kann diese Mail anschließend nur mit Hilfe des privaten Schlüssels des Empfängers. Der Nachrichtentransport ist sicher, weil der private Schlüssel nur auf dem Zielcomputer verfügbar ist und nie über das Internet übertragen wurde.

Damit das Verfahren funktioniert, müssen die Kommunikationspartner natürlich vor der ersten Verschlüsselung die jeweiligen öffentlichen Schlüssel austauschen. Da diese Schlüssel ohnehin frei zugänglich sind, kann der Austausch ohne große Risiken über das Internet erfolgen.

Darüber hinaus eignet sich das Paar aus öffentlichem und privatem Schlüssel zum Verifizieren des E-Mail- Absenders. In diesem Fall erstellen Sie mit Hilfe Ihres privaten Schlüssels eine Art digitale Unterschrift, die dann mit der Mail übertragen wird. Auf Empfängerseite dient Ihr öffentlicher Schlüssel dazu, die Unterschrift zu überprüfen. Wenn sich die Unterschrift verifizieren lässt, kann der Empfänger sicher sein, dass die Mail von Ihnen stammt und unterwegs nicht verfälscht wurde.

Wie Sie die Verschlüsselung in der Praxis einsetzen, erklären wir in den nächsten Teilen dieses Tipps.

Sicherer E-Mail-Versand dank Verschlüsselung, Teil 2
Versionen: Outlook 2013, 2010, 2007, 2003 und 2002/XP

Fast jeden Tag kommen neue Details ans Licht, wie die Geheimdienste den weltweiten Datenverkehr ausspionieren. Wenn Ihnen Ihre Privatsphäre lieb ist, sollten Sie zumindest Ihre E-Mails verschlüsseln. Das ist mit Outlook kein Problem, denn Outlook hat die nötigen Funktionen gleich eingebaut. In diesem mehrteiligen Tipp erfahren Sie, wie Sie sie effektiv einsetzen.

Aus dem ersten Teil wissen Sie, wie das asymmetrische Verschlüsselungsverfahren in Outlook funktioniert. Konkret basiert das S/MIME-Verfahren auf Zertifikaten nach dem X.509-Standard. Sie werden von autorisierten Zertifizierungsstellen (CA = Certificate Authority) ausgegeben und beglaubigt. Im Betriebssystem bzw. im Browser sind diese Zertifizierungsstellen als vertrauenswürdige Herausgeber hinterlegt, so dass die Echtheit eines X.509-Zertifikats jederzeit überprüft werden kann.

Es gibt allerdings verschiedene Zertifikatsklassen und nur in den höherwertigen Klassen werden Identitätsnachweise durch einen Personalausweis oder gar das persönliche Erscheinen verlangt. Die höhere Sicherheit lassen sich die Zertifizierungsstellen jedoch gut bezahlen.

Für einfache Zwecke genügt oft ein Zertifikat, in dem nur die Echtheit Ihrer E-Mail-Adresse verifiziert wird. Solche Zertifikate gibt es sogar kostenlos, wobei Sie in Kauf nehmen müssen, dass die Laufzeit auf ein Jahr beschränkt ist und Sie danach eine Verlängerung beantragen müssen.

Kostenlose Zertifikate stellen zum Beispiel die israelische Firma StartCom (<https://www.startssl.com/>) und die aus Großbritannien stammende Comodo Group (<https://secure.comodo.com/products/frontpage?area=SecureEmailCertificate>) aus. Die folgende Anleitung zeigt, wie Sie ein Zertifikat von Comodo auf Ihrem PC installieren.

1. Starten Sie den Internet Explorer, auch wenn Sie sonst einen anderen Browser verwenden. Mit dem Internet Explorer gelingt die Systemintegration des neuen Zertifikats besser als mit anderen Browsern.
2. Öffnen Sie die Webseite <https://secure.comodo.com/products/frontpage?area=SecureEmailCertificate>. Es kann sein, dass Sie der Internet Explorer in einer Leiste über der Webseite fragt, ob Sie das "Microsoft Certificate Enrollment Control" ausführen wollen. Stimmen Sie dem zu, indem Sie auf die Leiste klicken und im Kontextmenü *Add-On ausführen* anwählen. Danach klicken Sie auf *Ausführen*. Unter Umständen fragt Sie der Internet Explorer auch, ob er einen digitalen Zertifikatsvorgang ausführen soll. Beantworten Sie die Frage dann mit einem Klick auf *Ja*.
3. Auf der Antragsseite geben Sie Ihren Vor- und Nachnamen sowie Ihre E-Mail-Adresse ein. Im Feld *Country* müssen Sie den englischen Namen Ihres Heimatlandes auswählen - zum Beispiel "Germany".
4. Klicken Sie dann auf *Advanced Private Key Options*, um im danach eingeblendeten Bereich die *Key Size* auf "4096" zu ändern und das Kontrollkästchen *User protected?* einzuschalten. Die anderen Einstellungen des Bereichs lassen Sie unverändert.
5. Unter *Revocation Password* geben Sie ein Kennwort ein, das Sie im Notfall zum Widerrufen des Zertifikats verwenden können - etwa wenn der private Schlüssel in falsche Hände gelangt ist. Und wenn Sie auf den Comodo-Newsletter verzichten können, entfernen Sie das Häkchen im Kontrollkästchen *Opt in?*.
6. Blättern Sie dann nach ganz unten auf der Seite, um das Kontrollkästchen *I ACCEPT the terms of this Subscriber Agreement* anzukreuzen und auf *Next* zu klicken.
7. Die anschließende Zertifikatsanforderung in Ihrem Auftrag bestätigen Sie mit *Ja*.
8. Nun beginnt die Erstellung des Zertifikatsschlüssels. Bestätigen Sie das angezeigte Dialogfenster einfach mit *Ok*.
9. Am Ende sehen Sie im Internet Explorer eine Webseite mit dem Hinweis "Application is successful". Das Fenster des Browsers können Sie daraufhin schließen.

Nun warten Sie ab, bis Sie eine E-Mail von Comodo-"Certificate Customer Services" erhalten. Mit dieser E-Mail prüft Comodo, ob Sie auch wirklich der Besitzer der E-Mail-Adresse sind, die Sie in Ihrem Zertifikatsantrag angegeben haben. Ihr Zertifikat erhalten Sie nämlich erst, wenn Sie auf die E-Mail von Comodo reagieren. Was Sie tun müssen, erfahren Sie im nächsten Teil dieses Tipps.

Sicherer E-Mail-Versand dank Verschlüsselung, Teil 3
Versionen: Outlook 2013, 2010, 2007, 2003 und 2002/XP

In diesem mehrteiligen Tipp zeigen wir Ihnen, wie Sie Ihre E-Mail-Kommunikation durch Verschlüsselung sicherer machen. Inzwischen haben Sie ein kostenloses Zertifikat für Ihre E-Mail-Adresse beantragt. Nun geht es darum, Ihre Angaben gegenüber der Zertifizierungsstelle zu verifizieren. Wie das im Detail aussieht, verrät Ihnen der vorliegende Teil unseres Tipps der Woche.

Nachdem Sie ein kostenloses E-Mail-Zertifikat beantragt hatten, erhalten Sie per E-Mail eine Bestätigung von der Zertifizierungsstelle - in unserem Beispiel von Comodo. In der E-Mail erfahren Sie, welche Schritte erforderlich sind, um das Zertifikat auf Ihrem Computer zu installieren. Hier die genaue Vorgehensweise:

* Öffnen Sie in Outlook den Posteingang des Kontos, für das Sie ein Zertifikat beantragt haben.
* Suchen Sie nach einer E-Mail von Comodo-"Certificate Customer Services". Wenn der Internet Explorer Ihr Standardbrowser ist, können Sie darin einfach auf die Schaltfläche *Click & Install Comodo Email Certificate* klicken.

Wenn Sie standardmäßig einen anderen Browser verwenden oder sich nicht sicher sind, welcher Browser Ihr Standardbrowser ist, starten Sie jetzt den Internet Explorer und öffnen Sie darin folgende Webseite:
[**https://secure.comodo.com/products/!SecureEmailCertificate\_Collec2**](https://secure.comodo.com/products/%21SecureEmailCertificate_Collec2)

Auf der Seite geben Sie die E-Mail-Adresse ein, für die Sie das Zertifikat beantragt haben. Und im Feld *Collection Password* tragen Sie das "Collection Password" ein, das Ihnen in der E-Mail von Comodo mitgeteilt worden ist. Danach klicken Sie auf *Submit & Continue*.

* Es wird eine Zertifikatsanforderung in Ihrem Auftrag ausgeführt, weshalb Sie die entsprechende Frage mit *Ja* bestätigen.
* Nach erfolgreicher Installation des Zertifikats meldet die Comodo-Webseite: "Successful". Danach können Sie das Browserfenster schließen.

Das Zertifikat ist jetzt auf Ihrem Computer installiert. Allerdings weiß Outlook noch nichts davon. Darum sind weitere Schritte in Outlook erforderlich.

Vorab aber ein Hinweis für Benutzer von Outlook 2013 unter Windows 8. Der Einsatz von digitalen Zertifikaten funktioniert in dieser Konstellation nicht immer auf Anhieb. Zur Problemlösung hat Microsoft deshalb einen Hotfix herausgebracht, der über folgende Webseite erhältlich ist:

[**http://support.microsoft.com/kb/2813237/en-us**](http://support.microsoft.com/kb/2813237/en-us)

Klicken Sie auf *Hotfix-Download ist verfügbar* und geben Sie auf der nächsten Seite Ihre E-Mail-Adresse an, um sich einen Link zum Hotfix schicken zu lassen. Am besten speichern Sie das Hotfix-Paket auf Ihrer Festplatte. Führen Sie dann die heruntergeladene EXE-Datei aus, um die Setup-Datei zu entpacken. Diese MSU-Datei starten Sie anschließend per Doppelklick.

Nun aber zu den Schritten, mit denen Sie Ihr Zertifikat in Outlook aktivieren. Wir gehen davon aus, dass Sie in Zukunft all Ihre E-Mails verschlüsseln oder digital signieren wollen.

* Wählen Sie in Outlook 2013 und 2010 *Datei-Optionen* an, wechseln Sie dann zur Kategorie *Trust Center* (2013) bzw. *Sicherheitscenter* (2010) und klicken Sie dort auf die Schaltfläche *Einstellungen für das Trust Center* bzw. *…Sicherheitscenter*. Im danach angezeigten Dialogfenster wechseln Sie zur Kategorie *E-Mail-Sicherheit*.

In Outlook 2007 wählen Sie *Extras-Vertrauensstellungscenter* an und im zugehörigen Dialogfenster wechseln Sie zur Kategorie *E-Mail-Sicherheit*.

In Outlook 2003 und 2002/XP wählen Sie *Extras-Optionen* an und danach wechseln Sie auf die Registerkarte *Sicherheit*.

* Um E-Mails generell zu verschlüsseln und mit einer digitalen Signatur zu versehen, aktivieren Sie die Kontrollkästchen *Inhalt und Anlagen für ausgehende Nachrichten verschlüsseln* (2013, 2010, 2007) bzw. *Nachrichten und Anlagen verschlüsseln* (2003, 2002/XP) sowie (*Ausgehenden) Nachrichten digitale Signatur hinzufügen*. - Lassen Sie außerdem das Kontrollkästchen *Signierte Nachrichten als Klartext senden* aktiviert, damit Empfänger, die keine S/MIME-Zertifikate besitzen, weiterhin unverschlüsselte E-Mails von Ihnen erhalten können.
* Überprüfen Sie die Details des Verschlüsselungsverfahrens, indem Sie auf die Schaltfläche *Einstellungen* klicken.
* Üblicherweise enthält das nun angezeigte Dialogfenster die Angaben zu dem von Ihnen installierten Zertifikat. Mit den *Auswählen*-Schaltflächen im unteren Bereich können Sie testen, ob es sich wirklich um das gewünschte Zertifikat handelt und gegebenenfalls ein anderes Zertifikat auswählen. Zur Bestätigung der Angaben klicken Sie auf *Ok*.
* Schließen Sie alle geöffneten Dialogfenster mit *Ok*, bis Sie wieder im Outlook-Fenster angelangt sind.

Ab sofort fügt Outlook Ihren E-Mails automatisch eine digitale Signatur hinzu und versucht, Ihre E-Mails zu verschlüsseln. Das führt anfangs dazu, dass beim E-Mail-Versand eine Meldung über "Verschlüsselungsprobleme" erscheint.

Klicken Sie einfach auf *Unverschlüsselt senden* und machen Sie sich vorerst keine Gedanken darüber. Den Grund für die Meldung lernen Sie im nächsten Teil unseres Tipps kennen.

Sicherer E-Mail-Versand dank Verschlüsselung, Teil 4
Versionen: Outlook 2013, 2010, 2007, 2003 und 2002/XP

E-Mail-Verschlüsselung ist nicht nur für die interessant, die etwas zu verbergen haben. In Zeiten umfassender Geheimdienstüberwachung geht das Thema alle etwas an. Darum zeigen wir Ihnen in diesem mehrteiligen Tipp, welche Verschlüsselungsmethoden Outlook zu bieten hat. Mit dem kostenlosen E-Mail-Zertifikat, das Sie in den letzten Teilen beantragt und installiert haben, sind Sie fast am Ziel. Jetzt müssen Sie es nur noch effektiv einsetzen.

Wie Sie aus dem letzten Teil dieses Tipps wissen, fügt Outlook Ihren E-Mails automatisch eine digitale Signatur hinzu, die den öffentlichen Schlüssel Ihres Zertifikats enthält. Nur die Verschlüsselung gelingt noch nicht, so dass beim E-Mail-Versand ein entsprechendes Hinweisfenster erscheint.

Grund dafür ist, dass Sie noch keine öffentlichen Schlüssel der E-Mail-Empfänger besitzen, denn nur damit können E-Mails verschlüsselt werden. Sie müssen die Personen, mit denen Sie E-Mails austauschen, also dazu bringen, die gleichen Schritte wie Sie zu unternehmen: Zertifikat beantragen, installieren und den öffentlichen Schlüssel als digitale Signatur verteilen.

Wenn die Personen ebenfalls mit Outlook arbeiten, können Sie sie dabei mit Ihren Erfahrungen unterstützen. Ansonsten funktioniert das System nur, wenn Ihre Kommunikationspartner mit einem E-Mail-Programm arbeiten, das wie Outlook S/MIME-Unterstützung bietet. Das Einrichten der Zertifikate wird dann aber unterschiedlich sein.

Sobald das System etabliert ist, werden Sie immer mehr E-Mails mit einer digitalen Signatur erhalten. Diese Zertifikate müssen Sie den Einträgen in Ihrem Kontaktordner zuordnen, was am besten über einen Export/Import-Vorgang funktioniert:

1. Wenn eine E-Mail eine digitale Signatur enthält, signalisiert Outlook dies mit einem speziellen Symbol am rechten Rand des Nachrichtenkopfs. Klicken Sie auf dieses Symbol, um die Signatur zu prüfen und ein Dialogfenster mit dem Ergebnis zu öffnen.
2. Klicken Sie auf *Details*.
3. Damit öffnen Sie ein weiteres Dialogfenster mit Informationen über die Sicherheitsschichten. Markieren Sie die unterste Ebene mit dem Präfix "Signierer" und klicken Sie dann auf *Details anzeigen*.
4. Im nächsten Dialogfenster klicken Sie auf *Zertifikat anzeigen*.
5. Wechseln Sie auf die Registerkarte *Details* und klicken Sie dort auf *In Datei kopieren*.
6. Es öffnet sich ein Zertifikatexport-Assistent, in dem Sie auf *Weiter* klicken.
7. Als Exportformat übernehmen Sie die Standardeinstellung *DER-codiert-binär X.509 (.CER)*, indem Sie erneut auf *Weiter* klicken.
8. Unter welchem Namen das fremde Zertifikat gespeichert werden soll, bestimmen Sie nach einem Klick auf *Durchsuchen*. Danach fahren Sie mit einem Klick auf *Weiter* fort.
9. Klicken Sie auf *Fertig stellen*, um den Exportvorgang abzuschließen und bestätigen Sie die nachfolgende Meldung mit *Ok*.
10. Wechseln Sie nun in den Outlook-Kontaktordner und öffnen Sie den Kontakt, dessen Zertifikat Sie gerade in einer Datei gespeichert haben. Öffnen Sie ihn in Outlook 2013 in einem regulären Outlook-Kontaktformular und nicht in der Personen-Ansicht.
11. Wählen Sie in Outlook 2013, 2010 und 2007 *Kontakt-Anzeigen-Zertifikate* an. In Outlook 2003 und 2002/XP wechseln Sie im Kontaktformular auf die Registerkarte *Zertifikate*.
12. Klicken Sie auf die Schaltfläche *Importieren* und öffnen Sie dann die Zertifikatsdatei, die Sie in den vorherigen Schritten gespeichert haben.
13. Im Listenfeld *Zertifikate (digitale IDs)* erscheint daraufhin ein neuer Eintrag. Klicken Sie auf *Speichern & schließen*, um die erweiterten Kontaktinformationen zu speichern.

Outlook erkennt ab sofort automatisch, dass es einen öffentlichen Schlüssel für den jeweiligen Empfänger gibt. So werden die E-Mails an diesen Empfänger ebenfalls automatisch verschlüsselt.

Tipp: Wundern Sie sich nicht, wenn Outlook mitunter trotzdem die Meldung über "Verschlüsselungsprobleme" anzeigt. Dann werden Sie die E-Mail an mehrere Empfänger adressiert haben, wobei Ihnen von manchen Empfängern noch keine öffentlichen Schlüssel vorliegen. Nur diese Namen werden in dem Dialogfenster aufgelistet sein und nur diese Personen werden die E-Mail unverschlüsselt erhalten. Empfänger, denen Sie einen öffentlichen Schlüssel zugeordnet haben, erhalten die E-Mail selbstverständlich verschlüsselt.

Wenn Sie selbst eine verschlüsselte E-Mail erhalten, erkennen Sie das am Schloss-Symbol im Nachrichtenkopf, das neben dem Symbol der digitalen Signatur angezeigt wird.

Damit kennen Sie die wesentlichen Schritte zum Absichern Ihrer E-Mail-Kommunikation. Wenn Sie mehr wissen wollen - zum Beispiel über E-Mail-Verschlüsselung bei einer Synchronisierung mit dem Smartphone oder über das Alternativverfahren GnuPG -, besorgen Sie sich das SmartTools Sicherheitspaket für Outlook, das wir in Kürze für Sie bereitstellen. Es enthält nicht nur viele nützliche Tools, sondern auch ein eBook mit ausführlichen Informationen zu den einzelnen Verschlüsselungstechniken.