DATENSCHUTZPRAXIS

INTERVIEW MIT DEM FRAUNHOFER-INSTITUT FÜR SICHERE INFORMATIONSTECHNOLOGIE ZUM THEMA „VOLKSVERSCHLÜSSELUNG“

Michael Herfert und Jürgen Hartz

Hartz: Die fehlende sichere Verschlüsselung, während der E-Mail Verkehr ständig steigt, ist immer noch eine große Schwachstelle der elektronischen Kommunikation, nicht nur im privaten Bereich, sondern auch im geschäftlichen. Selbst viele Unternehmen versenden vertrauliche Informationen als offene E-Mail oder Dokumente, selbst mit sensiblen geschäftlichen oder gar Gesundheitsdaten, als unverschlüsselte Anlage.

Warum sind nach Ihrer Meinung die E-Mail Nutzer so wenig auf die Sicherheit beim E-Mail Verkehr bedacht?

Herfert: IT-Sicherheit entzieht sich der unmittelbaren Wahrnehmung. Wenn man mit seinem Web-Browser im Internet unterwegs ist, dann ist das Erlebnis unabhängig davon, ob der Browser eine sichere Verbindung über das TLS-Protokoll aufgebaut hat oder nicht. Ein Textverarbeitungsprogramm, das hellgraue Schrift vor einem weißen Hintergrund zeigt, würde niemand benutzen, weil die Mängel gravierend sind und unmittelbar wahrgenommen werden. Mängel in der IT-Sicherheit manifestieren sich oft erst viel später, etwa dann, wenn Firmengeheimnisse verloren gegangen sind oder personenbezogene Daten in falsche Hände geraten sind.

Hartz: Der neue elektronische Personalausweis, der verschiedene Zusatzfunktionen zum Beispiel für den elektronischen Einkauf beinhaltet, hat im Gegensatz zu anderen Ländern, die dies bei der Neueinführung von Ausweisdokumenten berücksichtigt haben, keine Möglichkeit, Dokumente zu verschlüsseln.

War die technische Hürde für die Installation eines sicheren E-Mail Zertifikates wie PGP oder S/MIME einfach zu hoch oder zu teuer?

Herfert: Ich bin ein großer Freund des neuen Personalausweises. Gerade in Bezug auf Datenschutz ist er vorbildlich. Es ist technisch möglich, ein S/MIME Zertifikat für eine digitale Signatur nachzuladen. Dafür gibt es zurzeit keinen Anbieter. Die Fähigkeit, Dokumente zu verschlüsseln, erhielte er aber auch dadurch nicht. Der neue Personalausweis entwickelt sich ja immer weiter, wer weiß was die Zukunft bringt.

Hartz: Das Fraunhofer-Institut für Sichere Informationstechnologie in Darmstadt hat zusammen mit der Telekom AG mit dem Projekt »Volksverschlüsselung« eine Initiative gestartet, eine sichere Verschlüsselung für »jedermann« bereitzustellen. Der BvD hat in seinen Fortbildungen bereits vor Jahren Seminarangebote zur Verschlüsselung inklusive Ausgabe eines persönlichen S/MIME-Zertifikates durchgeführt. Datenschutzbeauftragte sollten aufgrund ihrer Aus- und Weiterbildung über Mindestkenntnisse im IT-Bereich verfügen. Dennoch war nicht für alle die Installation des persönlichen Zertifikates unproblematisch. Offensichtlich stellt der Einsatz von sicherer Verschlüsselungstechnik mittels Zertifikaten, die ja in die Browser bzw. Mailprogramme eingebunden werden müssen, die Anwender vor Probleme.

Wie haben Sie diese Herausforderung umgesetzt?

Herfert: Wir haben mit der Volksverschlüsselungs-App eine Applikation für Microsoft Windows programmiert, die dem Nutzer alle schwierigen Schritte abnimmt. Er muss seine Mail-Adresse eingeben und einen Registrierungscode, den er zuvor von uns im Rahmen einer Identitätsfeststellung erhalten hat, und schon hat er Schlüssel sowie Zertifikate und sie sind auf seinem Rechner dort gespeichert, wo sie von den Applikationen erwartet werden. Es sind keinerlei weitere Konfigurationsschritte erforderlich. Die Schlüssel sind unmittelbar nutzbar.

Die Anforderung nach maximal einfacher Benutzbarkeit war von Anfang an ein hochpriorisiertes Ziel. Es war uns klar, dass wir als Informatiker das Erreichen dieses Ziels nicht selber beurteilen können. So haben wir wiederholt Nicht-Informatiker in den Entwicklungszyklus eingebunden, um tatsächlich »Usability by Design« zu erhalten.

Hartz: Können Sie uns in einfachen Worten erklären, warum das Zertifikat durch das Fraunhofer SIT eine wirklich sichere Möglichkeit der E-Mail Verschlüsselung darstellt?

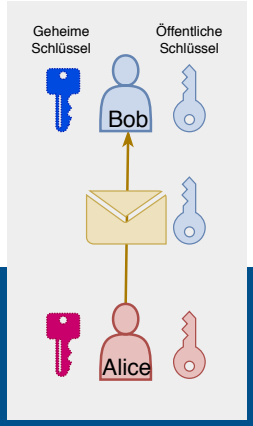

Abb.: Asymmetrische Verschlüsselung: Jeder Nutzer besitzt 2 Schlüssel,einen geheimen (links) und einen öffentlichen (rechts). Alice verwendet Bobs öffentlichen Schlüssel, um eine Nachricht für ihn zu verschlüsseln. Nur Bob kann sie mit seinem geheimen Schlüssel wieder entschlüsseln.

Herfert: Wir stellen nur dann ein Zertifikat aus, wenn wir uns von der Identität des Nutzers anhand eines Ausweisdokuments überzeugt haben. Auf das Übersenden einer Ausweiskopie oder gar die reine Überprüfung einer Mailadresse lassen wir uns nicht ein. Wer ein Zertifikat der Volksverschlüsselung nutzt, etwa über unseren Verzeichnisdienst, kann sicher sein, dass hinter diesem Zertifikat tatsächlich die im Zertifikat genannte Person steht.

Die eigentliche Verschlüsselung geschieht auf Basis etablierter, vollständig offen gelegter kryptografischer Algorithmen, die seit vielen Jahren im allgemeinen Gebrauch sind. Hinter solchen Algorithmen steckt meistens eine mathematische Operation, die in einer Richtung sehr einfach, in der anderen Richtung aber extrem schwierig ist. Es ist sehr einfach, zwei lange Zahlen zu multiplizieren, aber extrem schwierig, eine lange Zahl in ihre Primfaktoren zu zerlegen. Die Mathematiker suchen seit mehreren Jahrhunderten nach einem effizienten Algorithmus. Bis heute ohne durchschlagenden Erfolg.

Hartz: Da es sich bei dieser Verschlüsselung um eine echte Ende-zu-Ende-Verschlüsselung, also zwischen den jeweiligen Rechnern der Anwender, handelt, ist die Verschlüsselung hervorragend für Privatleute und für Einzelpersonen geeignet. In einer komplexen Unternehmensstruktur darf sie natürlich nicht eigenmächtig durch Mitarbeiter installiert werden, da damit IT Sicherheitsrichtlinien, wie zum Beispiel die interne E-Mail Archivierung, unterlaufen würden.

Wird auf diesen Umstand bei der Installation hingewiesen?

Herfert: Das Thema der Mail-Archivierung ist in der Tat schwierig. Das liegt daran, dass die entsprechenden Programme nicht auf Schlüssel eingestellt sind. Selbst die Hotlines der Hersteller sind hier oft überfragt – ein Indiz, dass solche Anfragen selten sind. Das liegt natürlich daran, dass es zu wenig Nutzer mit Schlüsseln gibt. Wir erwarten, dass sich dies ändert, wenn mehr Schlüssel verteilt sind. Bis dahin besteht ein sehr sinnvoller Workaround darin, dass die Firma eine Kopie des privaten Schlüssels anfertigt, um Nachrichten anstelle des Mitarbeiters entschlüsseln zu können. Das ist immer eine empfehlenswerte Strategie, auch ohne das Problem der Mail-archivierung. Der Zugriff auf diesen Schlüssel sollte durch organisatorische Regelungen präzise geregelt werden, um einen Missbrauch zu verhindern. Ein solches Vorgehen ist üblich und in meinen Augen im Businessbereich auch erforderlich.

Hartz: Derzeit muss der Antrag für ein Zertifikat persönlich gestellt werden. Die Person muss sich ausweisen. Auf diese Art ist die Möglichkeit, sich mal eben für ein Zertifikat zu registrieren, sehr eingeschränkt.

Welche Möglichkeiten wird es in Zukunft geben, schnell und einfach an ein Zertifikat zu kommen?

Herfert: Im Businessbereich bieten wir heute schon eine Identifizierung über eine Videokonferenz an. Dabei hält der Teilnehmer seinen Personalausweis in verschiedenen Winkeln in die Kamera, damit wir die Sicherheitsmerkmale überprüfen können. Das ist mit fast jedem Handy oder Tablet, den meisten Notebooks und den meisten externen Kameras möglich. Wir haben zudem Banken unter den Kunden, die das Recht haben, eigenständig Identifizierungen vorzunehmen. Auch Rechtsanwälte und Steuerberater können dieses Recht kostenfrei erhalten. In Kürze werden wir auch PostIdent anbieten, sodass wirklich jeder die Möglichkeit hat, Verschlüsselungszertifikate zu erhalten.

Hartz: Mit welchen Browsern und Mailprogrammen kann ich die Zertifikate problemlos verwenden? Gibt es Einschränkungen bei aktuellen Browsern und Mailprogrammen?

Herfert: Wir unterstützen Outlook, Thunderbird, Firefox, den Internet Explorer und Google Chrome. Dabei gibt es keine Einschränkungen.

Hartz: Auf welchen Systemen funktioniert die einfache, automatisierte Installation des Zertifikates derzeit?

Herfert: Wir haben mit Microsoft Windows begonnen, weil dies das Betriebssystem ist, welches die überwältigende Mehrheit der Nutzer verwendet. Wir planen Versionen für iOS und Android, danach auch für macOS und Linux. Zurzeit kann ich aber noch keinen belastbaren Fertigstellungstermin nennen.

Wer einmalig Zugriff auf ein Windows-System hat, etwa in einer virtuellen Maschine, um seine Schlüssel zu erzeugen, kann diese ▸

exportieren, um sie dann unter macOS oder Linux zu nutzen. Das ist durch die Nutzung internationaler Standards möglich, erfüllt aber nicht unseren Anspruch an Benutzungsfreundlichkeit. Wir empfehlen diese Möglichkeit daher den Experten.

Hartz: Kann man die Zertifikate auch auf mobilen Endgeräten installieren und nutzen?

Herfert: Für iOS ist dies durch ein spezielles Export-Format der Schlüssel, das von der Volksverschlüsselungs-App bereitgestellt wird, möglich. Auch dazu ist Handarbeit erforderlich, wie eben beschrieben. Wir haben das Vorgehen in Schritt-für-Schritt-Anleitungen dokumentiert. Den Anspruch an maximale Einfachheit wird aber erst die iOS- bzw. Android-Version der Volksverschlüsselungs-App erfüllen.

Hartz: Sind die vom Fraunhofer SIT ausgestellten Zertifikate mit den derzeitigen Standards voll kompatibel? Oder für die Tekkies: Welche Klasse oder Sicherheitsstufe erfüllen die vom Fraunhofer SIT ausgestellten Zertifikate? Für welche Zwecke können sie verwendet werden?

Herfert: Wir erstellen S/MIME-Zertifikate der Klasse 3, die für fortgeschrittene elektronische Signaturen benutzt werden können. Dabei weist Klasse 3 auf die persönliche Identifizierung hin, also die Ausweiskontrolle im Face2Face-Kontext. Die Signaturen sind fortgeschritten, aber nicht qualifiziert. Qualifizierte elektronische Signaturen sind manuellen Signaturen gleichgestellt. Entsprechende Zertifikate sind aber sehr teuer und haben sich bis heute, 22 Jahre nach Einführung des ersten Signaturgesetzes in Deutschland, nicht flächendeckend durchgesetzt. Meiner Meinung nach werden sie es auch nie tun. Fortgeschrittene Signaturen sind aber keineswegs wertlos, sie ersetzen nur nicht automatisch die manuelle Signatur. Insbesondere Prozesse in Firmen lassen sich mit ihnen sehr gut abbilden, sogar so, dass auch sehr strenge Revisionsabteilungen ihr Einverständnis geben.

Insgesamt kann man die Zertifikate für drei Zwecke verwenden: Zum Signieren, zum Verschlüsseln und für die Authentifizierung. Der letzte Punkt bietet noch ein unglaubliches Potenzial, denn er bedeutet, dass die Zertifikate im Browser genutzt werden können, um dort webbasierte Log-Ins mit Passwörtern abzulösen. Die Konfiguration eines Web-Servers zur Umstellung von Passwörtern auf kryptografische Schlüssel ist in den meisten Fällen sehr einfach, da die wichtigsten Server darauf vorbereitet sind. Für den Nutzer ergibt sich ein Gewinn an Sicherheit und gleichzeitig eine Vereinfachung der Benutzung, denn er muss keine neuen Passwörter setzen, keine verwalten und auch keine Passwörter unter seinen Geräten synchronisieren. Eine derartig erfreuliche Koinzidenz ist sehr selten im Bereich der IT-Sicherheit.

Hartz: Sichere Zertifikate müssen von einem Trust Center ausgegeben werden, damit diese als »vertrauenswürdig« akzeptiert sind. **Welches Trust Center stellt die Fraunhofer-Zertifikate aus? Und wie wird deren Sicherheit gewährleistet?**

Herfert: Wir haben unser eigenes Trustcenter aufgebaut und alle dazu notwendigen Maßnahmen ergriffen sowie die erforderlichen Dokumente verfasst. Das hatte den Vorteil, dass wir von niemandem abhängig waren und alle Schritte des Prozesses selber in der Hand hatten. Unser gesamtes Institut beschäftigt sich mit dem Thema IT-Sicherheit. Wir wissen sehr genau, wie ein solches System technisch und organisatorisch abzusichern ist.

Nachteilig für den Nutzer ist, dass unser Trustcenter vertrauenswürdig ist, aber nicht zu den im Betriebssystem vorinstallierten gehört. Bei der Installation der App erscheint eine Warnmeldung des Betriebssystems, die sich aus verständlichen Gründen nicht abschalten lässt. Wir arbeiten gerade an einer Kooperation mit einem Hersteller vorinstallierter Zertifikate. Noch in diesem Jahr wird die Warnmeldung dann verschwinden.

Hartz: Welche Ziele haben Sie sich mit der »Volksverschlüsselung« gesetzt? Wie viele Zertifikate wollen Sie unter das Volk bringen?

Herfert: Eine Zahl kann ich gar nicht nennen, aber die Möglichkeiten, Zertifikate zu nutzen, sollten sich verbessern. Mein Traum ist es, die Volksverschlüsselung in die Einwohnermeldeämter zu bringen. Dort gehört sie hin. Wir unterstützen gerne jedes Einwohnermeldeamt. Der Aufwand dort ist minimal.

Hartz: Herr Herfert, wir bedanken uns für das Interview und die Unterstützung in der Kooperation zwischen dem Fraunhofer-Institut für Sichere Informationstechnologie und dem BvD.

Der BvD hat seit April 2019 mit dem Fraunhofer-Institut für Sichere Informationstechnologie in Darmstadt, geleitet von Prof. Michael Waidner, eine Kooperation begründet. In gegenseitiger Zusammenarbeit wollen wir das Projekt »Volksverschlüsselung« weiter voranbringen und unseren Mitgliedern die Mailverschlüsselung auch in anderen Projekten wie zum Beispiel »Datenschutz geht zur Schule« vermitteln.

Das Fraunhofer-Institut hat beim Verbandstag im Juni in Berlin bereits vielen Mitgliedern ein kostenloses privates Zertifikat oder ein Zertifikat zur geschäftlichen Nutzung ausstellen können.

Das Zertifikat zur privaten Nutzung ist kostenfrei. Ein Zertifikat zur geschäftlichen Nutzung kostet 50 € jährlich.

Die nächste Möglichkeit für Mitglieder und Teilnehmer der direkten Registrierung und Ausstellung eines Zertifikates ist bei der Herbsttagung vom 23. bis 25. Oktober 2019 in Nürnberg.

Das Interview führte Jürgen Hartz, stellvertretender Vorstandsvorsitzender BvD, mit Michael Herfert, Abteilungsleiter Cloud Computing, Identity & Privacy am Fraunhofer-Institut für Sichere Informationstechnologie, Darmstadt.