Eine Themenbeilage der
Heise Medien GmbH & Co. KG

I
2015

SICHERHEIT & DATENSCHUTZ

Verschlüsselung, Authentifizierung und Public-Key-Infrastruktur

Access Control:
Was Biometrie heute schon leisten kann

OpenPGP für Unternehmen:
Wie Open Encryption für Firmen funktioniert

E-Mail Security:
Welche Gefahren mit der Post kommen

Smart Grids & Industrie 4.0:
Wann kritische Infrastrukturen sicher sind

Vertrauensnetzwerke:
Wem wir unsere Schlüssel anvertrauen dürfen

Public-Key-Infrastruktur:
Welche Aufgaben eine PKI übernehmen muss

powered by: TeleTrusT Pioneers in IT security. iX

Eine Veranstaltung von heise Events

5. Bremer IT-Sicherheitstag

Embedded Systems – eingebaute Sicherheit und Gefahrenabwehr

10. September 2015

Beim Internet der Dinge (IoT – Internet of Things) wachsen Informationstechnik und Produktion zusammen – Stichwort Industrie 4.0. Die Vernetzung von IT und Maschinen verlangt aber auch nach neuen integralen Sicherheitskonzepten, damit Systeme und Prozesse vor unbefugter Manipulation gesichert sind.

Ort: Hochschule Bremen, ZIMT

Inhaltliche Schwerpunkte:

- Industrie 4.0 – Wie Hacker in Industrie-IT eindringen können
- Automotive – Sicherheitslücken beim Connected Car
- Wartung von Embedded Systems
- Welche Anforderung stellt eine Versicherung an die IT-Sicherheit
- Wirtschaftsspionage – Daten und Fälle aus der Praxis
- Safety, Trust, Security & Hope

Teilnahmegebühr: 129,00 Euro (inkl. MwSt.)

Sponsoren: CONSIST Business Information Technology; TREND MICRO

Organisiert von: heise Events

In Zusammenarbeit mit: IS-BREMEN

Weitere Informationen und Anmeldung unter: **www.heise-events.de/5bremerITST**

Nutzen Sie die Möglichkeit zur PGP-Zertifizierung: **www.ct.de/pgp**

Digitale Souveränität

Liebe Leserinnen und Leser,

sind Sie digital souverän? Können Sie mit jedem Ihrer Geschäftspartner einfach, aber dennoch vertraulich kommunizieren? Sind Ihre täglich zu übermittelnden Daten ausreichend vor fremden Blicken geschützt?

In unserer durchdigitalisierten Gesellschaft sind sensible Daten ein begehrtes Gut und deshalb auch ständigen Gefahren ausgesetzt. Durch Schnüffelaktionen, Cyberkriminalität und allzu oft einfach durch Fehler bei der Absicherung kommen Daten abhanden und können anschließend durch Dritte verwertet werden. Auch der Gesetzgeber nimmt, unter anderem bedingt durch die sich etablierende Meldepflicht sicherheitsrelevanter IT-Vorfälle bei kritischen Infrastrukturen, Einfluss auf die Hoheit über Unternehmensdaten. Obwohl ein effizienter Schutz von Bestands- und Kommunikationsdaten zum Standard gehören sollte, besteht bei vielen Unternehmen, Organisationen und Institutionen noch dringender Nachholbedarf.

All diesen Herausforderungen zum Trotz ist aber digitale Souveränität möglich. Die IT-Sicherheitsbranche in Deutschland ist sehr gut aufgestellt und besitzt durch die starke deutsche Datenschutzgesetzgebung ein Alleinstellungsmerkmal. Die mittelständisch geprägte deutsche IT-Sicherheitswirtschaft gilt mit ihren Lösungen und Dienstleistungen als innovativ und wegweisend. „IT Security made in Germany“ steht wie ein Leuchtturm und strahlt über Deutschland hinaus.

Die vorliegende Beilage „Sicherheit & Datenschutz“ will Ihnen Einblick in ausgewählte Themen der IT-Sicherheit verschaffen, die uns als Bundesverband IT-Sicherheit derzeit beschäftigen. Unsere Artikel zielen dabei auf grundsätzliche Fragen ab, mit denen Sie sich als IT-Verantwortlicher beschäftigen müssen. Neben Alltagsproblemen kleiner und mittelständischer Unternehmen (KMU) mit der Verschlüsselung soll Ihnen das Themenfeld „E-Mail Security“ (S. 14) nähergebracht werden. Damit verbunden stellt sich die Frage, wie „Vertrauensnetzwerke“ (S. 33) dazu ihren Beitrag leisten können.

Außer der technischen Sicherheit spielt insbesondere der verantwortungsbewusste Umgang mit den eingesetzten Verschlüsselungstechnologien eine zentrale Rolle. Hierzu stellen wir Ihnen mit Beiträgen zu den Themen „OpenPGP für Unternehmen“ (S. 8), „Any-to-Any Encryption“ (S. 20) und „Public-Key-Infrastrukturen“ (S. 29) drei Konzepte vor, die Ihnen bei der Realisierung der Verschlüsselung in Ihrem Unternehmen helfen können.

Einen Schwerpunkt unserer aktuellen Arbeit bilden gegenwärtig auch die Herausforderungen des geplanten IT-Sicherheitsgesetzes und dessen Auswirkungen auf Unternehmen und kritische Infrastrukturen Dies wird in den Beiträgen zum „IT-Sicherheitsgesetz“ (S. 19) und zum Thema „Smart Grids & Industrie 4.0“ (S. 26) differenziert aufbereitet.

Weitere Praxisbeiträge, etwa zur technischen Zukunft der Gesundheitsfürsorge im Artikel „E-Health-Telematik“ (S. 11) sowie zu Anwendungsszenarien biometrischer Verfahren in Verbindung mit dem Thema „Access Control“ (S. 4), runden diese Beilage ab.

Wir möchten Sie mit unseren Beiträgen anregen, sich stärker mit Ihrer IT-Sicherheit zu beschäftigen: Bewahren Sie Ihre digitale Souveränität!

Dr. Holger Mühlbauer
TeleTrusT – Bundesverband IT-Sicherheit e.V. (Geschäftsführer)

Biometrie wird alltagstauglich

Automatisierte Erkennungssysteme lassen sich durch biometrische Verfahren zielgerichtet optimieren

Schon ein kurzer Blick in den Augensensor genügt: Biometrische Anwendungen bieten nicht nur den Benutzern von IT-Systemen mehr Komfort, sie steigern zugleich die Sicherheit von Zugangskontrollen. Denn zur Identitätsprüfung verwenden sie individuelle Merkmale – die man weder vergessen noch verlieren kann.

Unter Biometrie versteht man Messverfahren für die Wiedererkennung von Personen, international standardisiert in der ISO-Norm ISO-2382-37:2012. Die International Organization for Standardization (ISO) definiert dabei den Begriff *biometrics* wie folgt: „Automated recognition of individuals based on their behavioural and biological characteristics." Biometrische Verfahren analysieren also das Verhalten eines Menschen und/oder eine Eigenschaft seiner biologischen Charakteristika.

Bei diesen unterscheidet man zum einen anatomische Merkmale, die durch die Strukturen des Körpers geprägt werden (Fingerabdruck, Irismuster), und zum anderen physiologische Merkmale, die von Funktionen des Körpers abhängen, beispielsweise die menschliche Stimme. Eine biometrische Authentisierung ermöglicht somit die eindeutige Verknüpfung eines Individuums mit einer hinterlegten Identität, unabhängig davon, wo diese Identität gespeichert ist.

Unterschiedliche Authentisierungsverfahren

Biometrische Anwendungen sind entweder als Verifikations- oder als Identifikationssysteme ausgelegt. Bei Verifikationssystemen gibt der Nutzer eine Identität vor, zu der eine eindeutige Referenz existiert. Sofern das Erkennungssystem mit einem authentischen Dokument (z.B. einer Kundenkarte) kombiniert ist, kann darauf die biometrische Referenz (z.B. ein Passfoto) abgelegt sein. Für die Verifikation wird ein Vergleich mit genau diesem einen Referenzbild durchgeführt (1:1-Vergleich).

Identifikationssysteme vergleichen hingegen das erfasste Bild mit vielen eingelernten Bildern und ermitteln aus dieser Menge das optimal passende Muster (1:n-Vergleich). Die Übereinstimmungen zwischen beiden Bildern müssen ein definiertes Mindestmaß erreichen, damit eine zuverlässige Zuordnung der mit dem Referenzbild verbundenen Identität möglich ist. Die Authentisierung, also der Identitätsnachweis des Nutzers, läuft nach folgendem Schema ab: Erfassung der biologischen Charakteristika mit geeigneten Sensoren – Vorverarbeitung zur Datenverbesserung – Merkmalsextraktion zur signifikanten Beschreibung der Muster – Vergleich der Merkmale mit den vorab gespeicherten Referenzdaten.

Biometrisch relevante Merkmale

Der Aufbau eines biometrischen Systems erfordert nicht nur die Auswahl passender technischer Komponenten (Sensor, Signal Processing Subsystem, Comparison Subsystem und Decision Subsystem). Es muss auch ein geeignetes biometrisches Charakteristikum gefunden werden, das folgende Eigenschaften erfüllt: *Verbreitung* (Jede natürliche Person sollte das Charakteristikum aufweisen.); *Einzigartigkeit* (Es ist für jede Person unterschiedlich.); *Beständigkeit* (Es bleibt auf Dauer unverändert.); *Messbarkeit* (Es ist mit wenig Aufwand präzise messbar.); *Performanz* (Es ermöglicht eine gute Erkennungsleistung auch bei geringem Einsatz von Algorithmen.); *Sicherheit* (Es lässt sich nur schwer durch Replikate fälschen.); *Akzeptabilität* (Die Erkennungsmethode wird von der Zielgruppe angenommen.) Falls einzelne Kriterien in einem mono-modalen System nicht erfüllt werden, bieten multi-modale Systeme eine Lösung. So kann man beispielsweise eine Gesichtserkennung mit einer Iriserkennung verbinden, um auf diese Weise eine ausreichende Erkennungsleistung des biometrischen Systems zu erzielen.

Viele individuelle Merkmale sind allerdings genetisch oder durch Verhalten und Umwelt bedingt. Das Gesicht eines Menschen ähnelt nicht selten dem Aussehen seiner Eltern. Ebenso wird ein bestimmtes Verhalten, etwa der Gang oder die Art zu sprechen, häufig von den Eltern übernommen, aber auch im Laufe des Lebens von anderen Vorbildern adaptiert. Ein geeignetes biometrisches Charakteristikum sollte deshalb in erster Linie unter dem Einfluss von Zufallsfaktoren entstanden sein. Das gilt etwa für die Ausbildung eines Fingerabdrucks oder der Iris. Beide entstehen bereits in der Schwangerschaft zufällig, ihre Strukturen bleiben beständig und verändern sich auch während der Entwicklung zum Erwachsenen nicht mehr.

Technische Kriterien eines biometrischen Systems

Neben den biometrischen Charakteristika lassen sich auch die Mess- und Auswerteverfahren nach bestimmten Kriterien bewerten. Die folgenden Beispiele qualitativer Kategorien sollen verdeutlichen, welche Eigenschaften bei der Wahl des passenden Kontrollsystems eine Rolle spielen können.

Statisch/Dynamisch: Eine biologische Charakteristik kann oft ebenso einfach wie ein Schnappschuss aufgezeichnet werden (z.B. ein Foto des Gesichtes). Mitunter ist aber auch die kontinuierliche Messung eines Signals notwendig (z.B. eine Aufzeichnung der Sprache oder des Tastaturverhaltens).

Kooperativ/Nicht kooperativ: Diese Kategorie, oft auch vereinfachend als Aktiv/Passiv bezeichnet, unterscheidet zwischen Messverfahren, bei denen die zu überprüfende Person wissentlich mit dem Sensor interagiert (z.B. beim Fingerabdruck) und denjenigen, bei denen sie sich der Erfassung gar nicht bewusst ist (z.B. bei der Videoüberwachung).

Kontaktfrei/Kontaktbehaftet: Bei einigen Modalitäten (z.B. bei Fingerbildern) ist eine Aufzeichnung sowohl kontaktfrei, etwa über ein digitales Foto, oder kontaktbehaftet, beispielsweise über einen Finger-

Ultimativer Schutz für alle digitalen Endgeräte – Kaspersky Lab kümmert sich darum

Die Bedrohung aus dem Internet hat sich in den vergangenen Jahren stark gewandelt. Heute werden nicht mehr nur Windows-PCs angegriffen, sondern immer öfter auch Smartphones und Mac-Rechner.
***Kaspersky Total Security – Multi-Device* ist ein umfassendes Sicherheitspaket, das PCs, Notebooks, Macs und Android-Smartphones sowie – Tablets schützt.**

Die Zeiten, als Cyber-Kriminelle auf albernen Schabernack aus waren und Viren programmiert haben, die mit mehr oder minder lustigen Sprüchen und bunten Einblendungen auf sich aufmerksam machten, sind lange vorbei. Es gibt auch praktisch keine Schädlinge mehr, die wahllos Daten löschen oder ohne Grund die Festplatte neu formatieren. Aktuelle Malware will stattdessen vor allem eines: nicht auffallen und still und heimlich ihr Werk verrichten.
Die Gründe für diesen Wandel liegen auf der Hand. Während es den Übeltätern früher darum ging, neue Tricks und Techniken auszuprobieren und Anerkennung von anderen Hackern zu erhalten, wollen sie heute mit ihrem Schadcode reich werden. Dazu locken sie die Anwender zum Beispiel auf gefälschte Webseiten und klauen dort persönliche Daten. Diese werden dann missbraucht, um unter dem Namen der Opfer einzukaufen oder um ihr Konto leer zu räumen. Außerdem setzen die Kriminellen immer häufiger versteckte Trojaner ein, die auf den Computern der Anwender schnüffeln oder von dort heimlich neue Spam-Nachrichten an die Kontakte aus dem Adressbuch des PC-Nutzers versenden. Mitunter verschlüsseln Cyber-Kriminelle auch Dokumente und Fotos auf der Festplatte. Um wieder an ihre Daten zu kommen, sollen die Opfer dann ein Lösegeld zahlen.

Smartphones sind bevorzugte Ziele

Aber damit nicht genug: Der Siegeszug von Smartphones und Tablets hat zu einem neuen Bedrohungsszenario für Anwender geführt. So hat sich laut einer Studie von Kaspersky Lab die Zahl der Cyber-Attacken auf Android-Nutzer im vergangenen Jahr verdreifacht. Fast jeder zweite dieser Angriffe hatte es auf die Finanzen der Anwender abgesehen – entweder durch das Versenden kostenpflichtiger SMS oder durch den versteckten Einsatz von Banking-Trojanern. Letztere Schädlinge ersetzen zum Beispiel die Eingabefelder in verbreiteten Banking-Apps und klauen dann Anmelde- oder Kreditkartendaten. Die Experten von Kaspersky Lab haben sogar eine Android-Malware identifiziert, die mTANs ausspioniert und an ihre Erzeuger weiterleitet. Mit diesen mTANs können die Kriminellen dann eigene Überweisungen erstellen.

Veränderungen in der privaten IT

Längst ist in Privathaushalten nicht mehr nur ein einzelner Desktop-PC mit dem Internet verbunden. Laut einer Umfrage von B2B International und Kaspersky Lab besitzt eine Familie durchschnittlich rund fünf internetfähige Geräte. 92 Prozent der befragten Nutzer speichern persönliche Daten auf ihren Computern und Smartphones. Ein herkömmlicher Virenscanner auf dem Desktop-Rechner kann die mobile Hardware aber nicht vor Schädlingen bewahren. Anwender benötigen stattdessen heute eine umfassende Sicherheitslösung, die alle ihre mit dem Internet verbundenen Geräte schützt.

Plattformunabhängiger Schutz für alle Bereiche des digitalen Lebens

Kaspersky Total Security – Multi-Device ist die ideale Lösung für diese Aufgabe. Die Software-Suite schützt Anwender auf allen wichtigen Plattformen. Dabei macht es keinen Unterschied, ob Total Security auf Windows-PCs, Mac-Rechner oder Android-Geräte eingesetzt wird. Die Lizenzen können auch jederzeit von einem Gerät auf ein anderes übertragen werden, wenn Sie sich etwa ein neues Smartphone gekauft haben.
Zur Verwaltung der Lizenzen genügt es, das My-Kaspersky-Konto aufzurufen und diese neu zuzuteilen. Im My-Kaspersky-Konto ist es auch möglich, den Sicherheitsstatus der angemeldeten Geräte online zu überprüfen und gegebenenfalls Maßnahmen zu ergreifen, um einen optimalen Schutz zu gewährleisten.

Einer für alles

Kaspersky Total Security – Multi-Device bewahrt Endgeräte vor Malware und eignet sich zum Schutz von Privatsphäre, Finanzdaten, Identität, Fotos und Dateien vor den Gefahren aus dem Internet. Die Software verfügt nicht nur über die klassischen Bestandteile wie Antivirus, Firewall und Kindersicherung, sondern auch über zahlreiche weitere Funktionen. Dazu zählen unter anderem Kaspersky Password Manager zum Erstellen und Verwalten von sicheren Passwörtern für Online-Konten und Webseiten, ein Online-Backup-Tool, ein Werkzeug zum Verschlüsseln privater Daten, eine Funktion zum sicheren Vernichten vertraulicher Dateien und eine virtuelle Tastatur zum Schutz vor Keyloggern. Aber die Sicherheits-Suite leistet noch mehr. So unterschätzen viele Anwender die Gefahr, die von der Webcam im Notebook ausgeht. Ohne dass sie es bemerken, können sie von Kriminellen auch in privatesten Momenten beobachtet werden. *Kaspersky Total-Security – Multi-Device* bietet deswegen die Möglichkeit, den Zugriff auf die Webcam zu sperren und nur dann zuzulassen, wenn Sie es wirklich wollen. Besonders praktisch ist auch der Aktivitätsmonitor, der Ihren Rechner überwacht und es so ermöglicht, schädliche Aktionen rückgängig zu machen.
Last but not least sorgt die Kaspersky-Funktion „Sicherer Zahlungsverkehr" dafür, dass Ihre Konto- und Kreditkartendaten geschützt sind, wenn Sie sie im Internet verwenden wollen. In dem speziellen abgesicherten Modus führen Sie Ihr Online-Banking und -Shopping sicher vor Betrügern aus. Die Funktion schützt Sie außerdem auch vor Phishing-Seiten, die aussehen wie die echte Webseite Ihrer Online-Bank, aber nur darauf aus sind, Ihre Login-Daten, PINs und TANs abzugreifen.

Fazit

Mit *Kaspersky Total Security – Multi-Device* erhalten Sie eine umfassende Sicherheitslösung, die Sie, Ihre Familie und die von Ihnen eingesetzten internetfähigen Geräte in allen digitalen Bereichen effektiv und gleichzeitig flexibel vor Bedrohungen aus dem Internet schützt. Und zwar gleichgültig, ob es sich um Windows-Computer, Mac-Rechner oder Android-Smartphones und -Tablets handelt.

Mehr Informationen dazu im Web: **www.kaspersky.de/total-security**.

abdrucksensor, möglich. Die Wahl der Methode hat dabei nicht nur Auswirkungen auf die Erfassung (z.B. bei einer möglichen Deformation des Fingers durch den Druck beim Auflegen auf den Sensor), sondern kann auch die Akzeptanz des Verfahrens beeinflussen (z.B. durch die Angst vor Krankheitsübertragungen).

Offen/Geschlossen: Komplexe biometrische Systeme, wie zum Beispiel die forensischen Anwendungen der Kriminalämter, sind in der Regel offen gestaltet, damit verschiedene Dienststellen die Daten in einem einheitlichen standardisierten Format untereinander austauschen können. Auch die derzeitigen Grenzkontrollanwendungen, wie das EasyPASS-System an vielen deutschen Flughäfen, sind offene Systeme. Schließlich muss der Zoll auch ein Personaldokument, das außerhalb Deutschlands ausgestellt wurde, bei der Einreise auslesen können. Das Speichern von biometrischen Daten im Pass in einem Standardformat ist dafür eine zwingend notwendige Voraussetzung. Ein Unternehmen, das seine Zugangskontrolle über biometrische Verfahren sicherstellen möchte, kann aber auch ein geschlossenes und proprietäres Speicherformat einsetzen. Dabei ergibt sich allerdings ein hohes Risiko: Falls der Systemanbieter vom Markt geht, müssen alle Referenzdaten umkodiert oder sogar neu erhoben werden.

Betreut/Nicht betreut: Bestimmte biometrische Systeme, wie etwa die der Grenzkontrollen, werden bewusst nur unter ständiger Betreuung betrieben. Einige Sensoren zeichnen sich aber durch gute Sicherheitseigenschaften aus und lassen sich nicht durch Artefakte (d.h. Fälschungen oder Plagiate einer Charakteristik) täuschen. Solche Sensoren sind beispielsweise für nicht betreute Systeme bei der physikalischen Zugangskontrolle zu Gebäuden geeignet, denn sie verringern spürbar den Personalaufwand. Onlinebanking-Systeme mit Biometrie stellen in der Regel ebenfalls nicht betreute Anwendungen mit hoher Relevanz dar.

Selbstverständlich gibt es noch weitere wichtige Aspekte bei der Auswahl eines geeigneten biometrischen Erkennungssystems. So reagieren etwa viele biometrische Verfahren empfindlich auf Störungen aus der Umgebung. Ein Gesichtserkennungssystem kann oft nur schwer mit direktem Sonnenlicht umgehen. Ein Sprechererkennungssystem hingegen bekommt womöglich in der Nähe einer viel befahrenen Straße Probleme.

Ausschlaggebend können auch die Beschaffungskosten sowie Aufwand und Kosten beim Betrieb des Systems sein. Nicht zuletzt zählt eine möglichst unkomplizierte Bedienbarkeit aller Komponenten. Ein Gesichtserkennungsfoto lässt sich zwar ohne viel Einweisung aufnehmen, gegebenenfalls muss aber der Betreuer angelernt werden, damit er auf gute Lichtverhältnisse und ähnliche Qualitätsmerkmale achtet. Manchmal ist auch ein Training der zu überprüfenden Personen selbst notwendig, beispielsweise bei einem Unterschriftenerkennungssystem. Das blinde Schreiben auf dem Touchscreen eines Tablet-PCs ist durchaus gewöhnungsbedürftig. Es kann dauern, bis eine weitgehend fehlerfreie Interaktion möglich ist.

Stärken und Schwächen biometrischer Verfahren

Worin liegen nun die Vorteile einer biometrischen Authentisierung? Die klassischen Mechanismen, beispielsweise die Wissensauthentisierung mit einem Passwort oder die Authentisierung über Token (Schlüssel), weisen eindeutige Nachteile auf: Passwort und Token lassen sich recht einfach unter Missachtung von Sicherheitsrichtlinien weitergeben, man kann sie vergessen oder verlieren. Um bei der ständig steigenden Zahl logischer und physikalischer Zugangskontrollen einem Verlust vorzubeugen, wählen die Anwender oft ungeeignete Speicherorte oder identische Passworte. Im Gegensatz dazu kann man biometrische Charakteristika nicht vergessen, und man kann sie auch nicht delegieren. Die Biometrie ist also in der Lage, solch grundlegende Probleme anderer Authentisierungsverfahren zu lösen.

Biometrische Verfahren kommen in der Regel dort zum Einsatz, wo man die Benutzbarkeit eines technischen Systems verbessern (z. B. Fingerprint-Authentisierung beim Smartphone) oder die Sicherheit des Systems steigern will. Allerdings können sich mit der Einführung einer biometrischen Nutzererkennung auch neue Sicherheitsrisiken ergeben. Besondere Bedeutung haben deshalb die Absicherung des Zugriffs auf den Datenspeicher und die Vermeidung möglicher Angriffe auf die zentrale verwundbare Mensch-Maschine-Schnittstelle, den Sensor.

So werden etwa die Defizite eines 2D-Gesichtserkennungsverfahrens deutlich, wenn ein vor die Kamera gehaltener Papierausdruck die Textur des Gesichtes in ausreichender Qualität für den Sensor reproduziert. Abhilfe leistet hier aber eine dreidimensionale Vermessung der Gesichtsoberfläche. Eine ähnliche Schwäche gegenüber Angriffen mit Artefakten (d.h. Replikaten) gilt auch für die Fingerbilderkennung. In diesem Fall kommt erschwerend hinzu, dass analoge Repräsentationen der biometrischen Charakteristik häufig unbeabsichtigt auf unterschiedlichsten Gegenständen hinterlassen werden. Fingerabdrücke in guter Qualität bleiben allzu oft auf glatten Oberflächen wie Gläsern, aber auch auf CD-Hüllen oder Touchscreens haften, und sie lassen sich ohne großen Aufwand kopieren. Danach ist es nur noch ein kleiner Schritt, einen Silikonfinger herzustellen und damit optische oder kapazitive Sensoren zu täuschen.

Fazit

Biometrische Verfahren können automatisierte Erkennungssysteme entscheidend verbessern. Um sie noch alltagstauglicher zu machen, ist die Entwicklung von überwindungssicheren Sensoren dringend erforderlich – und zum Beispiel unter Verwendung der „Optical Coherence Tomography“ auch möglich. Einstweilen sollten Sensoren zur Erfassung von biometrischen Merkmalen wie denen des Fingers durch zusätzliche Messverfahren (wie z.B. Venenerkennung) ergänzt werden.

Prof. Dr. Christoph Busch
Fraunhofer IGD, Leiter der AG Biometrie

TELETRUST-ARBEITSGRUPPE BIOMETRIE

Die TeleTrusT-Arbeitsgruppe „Biometrie“ bietet eine offene Plattform für den regelmäßigen Informations- und Erfahrungsaustausch zum Thema Biometrie. Ziel der Arbeitsgruppe ist der interdisziplinäre Dialog zwischen Technologie-Entwicklern, Datenschützern, Forschern, Behörden und Anwendern sowie eine objektive Diskussion über Stärken und Schwächen der Biometrie. Die Arbeitsgruppe identifiziert aktuelle Anwendungen und präsentiert neue Forschungsergebnisse und Produkte. Getragen wird die Plattform von TeleTrusT – Bundesverband IT-Sicherheit e.V., www.teletrust.de.

Ansprechpartner: Christoph Busch – Leiter der AG Biometrie (christoph.busch@igd.fraunhofer.de); Georg Hasse – Stellv. Leiter der AG Biometrie (georg.hasse@secunet.com); Alexander Nouak – Stellv. Leiter der AG Biometrie (alexander.nouak@igd.fraunhofer.de).

Big-LinX® The Remote Service Cloud

IT Security & Management
Industrielösungen für Profis

Big-LinX® The Remote Service Cloud **Die sichere Fernwartungslösung für Maschinen und Anlagen**
Die Remote Service Cloud Big-LinX bietet ein in Deutschland betriebenes Rechenzentrum zur sicheren Ferndiagnose und Fernwartung von Maschinen und Anlagen via Internet und Mobilfunk. Zu jeder Zeit weltweit im Einsatz für Anwendungen auf Schiffen, bei Energieversorgern, im Maschinenbau und in vernetzten Fertigungsanlagen. Technologie 100% made in Germany.

Big-LinX Vorteile
- Stabile Plattform seit Jahren mit zahlreichen namhaften industriellen Referenzkunden im Einsatz
- Als Cloud Service verfügbar, keine Investitionen in Rechenzentren und Personal notwendig
- Einfache Bedienung und Administration
- Höchste Sicherheit durch Nutzung von 2-Faktor Authentifizierung mit Smartcards bei jedem angebundenen System und Benutzer
- Offenes System, auch für Hardware anderer Hersteller

Neu: verteilte Datenerfassung für die Industrie 4.0
Entwickeln Sie eigene Apps auf den Router der IRF2000 zur flexiblen Erfassung und Auswertung von Daten in Java und übertragen Sie diese sicher per Smartcard authentifiziert und verschlüsselt in Ihre eigene zentrale Datenbank.

Testkit für PC Systeme (98,– €)
- 2 USB-Reader mit je einer Smartcard für Personal und Anlage
- Big-LinX Remote Client für Windows
- 6 Monate kostenlose Nutzung www.big-linx.de

Testkit für IRF2000 Router (495,– €)
- USB-Reader mit einer Smartcard für Personal
- IRF2200 GBit VPN Router für Hutschienenmontage inkl. Smartcard
- 6 Monate kostenlose Nutzung www.big-linx.de

Unterstützte Endgeräte
ads-tec Router und Firewalls der IRF2000 Serie optional mit Mobilfunk. Zur sicheren Anbindung von ganzen Netzwerken oder als Mobilfunkteilnehmer.

Unterstützte Endgeräte
Offene PC-Systeme sicher per Smartcard authentifiziert mit Big-LinX verbinden. Optimal für die Anbindung kleiner Anlagen an Big-LinX.

ads-tec GmbH
Germany
Telefon +49 7022 2522-200
sales@ads-tec.de
www.ads-tec.de

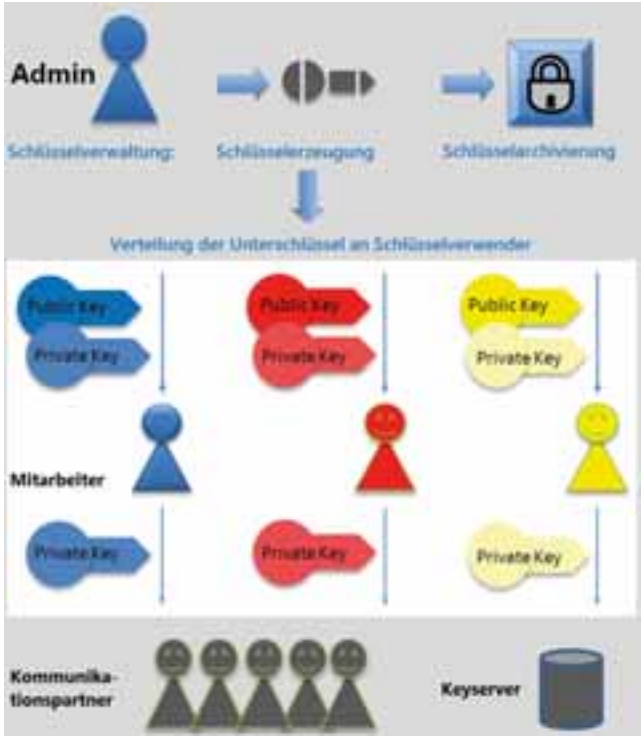
Leitfaden für eine effiziente E-Mail-Verschlüsselung

Die Einrichtung von OpenPGP-Schlüsseln ist weniger aufwendig, als oft behauptet wird

Wer als Verantwortlicher im Unternehmen über eine Verschlüsselung nach OpenPGP-Standard nachdenkt, hat bereits einen entscheidenden Schritt in Richtung sicherer E-Mail-Kommunikation getan. Je besser die Einführung geplant ist, desto reibungsloser funktioniert der Einsatz in der Praxis.

So viel vorab: Nur wer weiß, wogegen er sich schützen möchte, kann die richtigen Schutzmaßnahmen treffen. Will man Kundendaten sicher verwahren, Geheimdienste und Wirtschaftsspione aussperren, gesetzliche Datenschutzregelungen einhalten oder einfach nur den Anschluss nicht verlieren? Und wie steht es mit den Mitarbeitern: Wie stark sind sie in diesen Bereichen sensibilisiert, und welche Erfahrungen rund um Verschlüsselung bringen sie schon mit? Gerade Letzteres kann entscheidend dafür sein, wie komplex das einzusetzende Werkzeug sein darf und welcher Schulungsaufwand womöglich nötig sein wird.

Zunächst gilt es zu klären, ob eine Schlüsselhierarchie eingesetzt werden soll, wer die Schlüssel im Unternehmen erstellen und verwalten darf, wie sie archiviert werden und welche Schlüssel welchem Sicherheitsniveau unterliegen. Das Sicherheitsniveau wird bei jeder Implementation von OpenPGP neu definiert. Das höchste Level erreicht ein OpenPGP-Schlüssel nur dann, wenn er auf einem sehr sicheren System erzeugt wurde und der geheime Schlüssel dieses entweder nie verlassen hat oder bis zum nächsten Einsatz auf einem sicheren Datenträger verwahrt bleibt. Ein Beispiel wäre ein Live-Betriebssystem und ein USB-Stick, der nur an dieses System angeschlossen wird und sonst in einem Tresor liegt.



Quelle: Hans-Joachim Giegerich

Eine Schlüsselverwaltung übernimmt die Verteilung und Archivierung der OpenPGP-Schlüsselpaare.

Schlüssel richtig aufbauen und archivieren

Zu einem OpenPGP-Schlüsselpaar gehören wenigstens eine, häufig auch mehrere User-IDs. Die User-ID verrät, welcher Person (oder Gruppe) der Schlüssel zugeordnet ist. Sie besteht üblicherweise aus dem vollständigen Namen des Schlüsselinhabers sowie seiner E-Mail-Adresse. Optional gibt es ein Kommentarfeld, etwa zur Eingabe des Firmennamens. Durch mehrere User-IDs kann der Schlüssel verschiedenen E-Mail-Adressen zugeordnet werden. Häufig verwendet wird auch die Freeform-User-ID. Sie beinhaltet keine E-Mail-Adresse, sondern dient als eine Art Basis. Fügt man die E-Mail-Adresse des künftigen Benutzers dann als zusätzliche User-ID hinzu, kann man sie bei späteren Änderungen widerrufen, ohne dass dabei der gesamte Schlüssel zurückgezogen werden müsste. Aus arbeits- und datenschutzrechtlichen Gründen sollten Unternehmen übrigens eine klare Trennung zwischen beruflicher und privater Verwendung des Unternehmensschlüssels einhalten.

In heutigen Desktop-Umgebungen wirkt sich die Schlüssellänge kaum noch auf die Performance aus. Sie sollte daher so hoch wie möglich angesetzt werden (4096 Bit). Anders sieht es bei Schlüsseln für Mobilgeräte, Smartcards oder automatisierte Systeme aus, die sehr viele Daten in kurzer Zeit verarbeiten müssen. Hier empfiehlt sich eine Schlüssellänge von 2048 Bit, weniger (1024 Bit) ist nicht ratsam.

Das Sichern von Schlüsseln ist ein essenzieller Schritt beim Einsatz im Unternehmen. Im einfachsten Fall werden die Schlüssel der Mitarbeiter mit einer bekannten Passphrase von einer zentralen Stelle im Unternehmen ausgestellt und gleichzeitig archiviert. In weniger idealen Fällen muss den Schlüsseln eine – der archivierenden Stelle bekannte – Passphrase gesetzt werden, bevor sie gesichert werden. Die Auswahl des Sicherungsmediums legt fest, wie schnell im Problemfall der oder die Schlüssel wiederhergestellt werden können; sie hat auch direkten Einfluss auf die Haltbarkeit. Eine Archivierung auf Papier ist zwar praktikabel, aber vergleichsweise zeitaufwendig und fehleranfällig. Schneller geht es mithilfe eines ebenfalls sicher verschlüsselten Containers.

Für Unternehmen ist eine Schlüsselhierarchie in jedem Fall sinnvoll. Sie erleichtert den Mitarbeitern den Umgang mit OpenPGP, da beispielsweise ein Administrator die Zertifizierung von Schlüsseln (häufig auch signieren oder unterschreiben genannt) zentral durchführen kann. Hierzu wird ein Unternehmensschlüssel verwendet, der keiner spezifischen E-Mail-Adresse zugeordnet ist (Freeform-ID), sondern das Unternehmen als Ganzes repräsentiert. Mit diesem, möglichst auf hohem Niveau erzeugten Unternehmensschlüssel werden die Zertifizierungen der Mitarbeiterschlüssel sowie eingehender öffentlicher Schlüssel nach entsprechender Prüfung durchgeführt. Durch das Vertrauen der Mitarbeiter in den Firmenschlüssel bildet sich eine Zertifizierungskette vom einzelnen Mitarbeiter bis hin zum fremden Schlüssel. Auf diese Art lassen sich darüber hinaus auch gefälschte Schlüssel leichter erkennen.

Für das eingesetzte Schlüsselmaterial sollte man eine Schlüsselrichtlinie definieren. Diese besteht üblicherweise aus drei Teilen und fasst viele der Festlegungen je Schlüssel (oder einer Gruppe von Schlüsseln) zusammen. Dazu gehören das Sicherheitsniveau (Wie sicher wird ein Schlüssel aufbewahrt/verwendet?), der Zweck des Schlüssels (Wofür und wie wird der Schlüssel verwendet?) und die Zertifizierungsrichtlinie (Wie detailliert geht man beim Zertifizieren fremder Schlüssel vor?). Ohne Zertifizierungsrichtlinie ist der Schlüssel nicht für öffentliche Zertifizierungen geeignet.

Kurze Anleitung zur Schlüsselerzeugung

Für die Erstellung sicherer Schlüssel sind folgende Komponenten entscheidend: eine kryptografisch sichere Passphrase, eine Freeform-User-ID, User-IDs mit Angabe des vollen Namens und der E-Mail-Adresse des Benutzers, eine Schlüssellänge von mindestens 2048 Bit (besser 4096 Bit), ein Ablaufdatum von maximal fünf Jahren und ein Offline-Hauptschlüssel. Beim Format der User-IDs gilt es zu beachten, dass aus Sicherheitsgründen viele OpenPGP-Anwender nur User-IDs zertifizieren, deren Name mit den Angaben auf dem Personalausweis zu 100 % übereinstimmt. Die Generierung des Unternehmensschlüssels sollte unbedingt mit hoher Sicherheit, also in einem sicheren Live-Betriebssystem ohne Internet-Verbindung stattfinden. Hierfür kommt ein GnuPG in aktueller Version am ehesten in Betracht. Nach Eingabe von > gpg –gen-key in die GnuPG-Kommandozeile sieht der Schlüssel in etwa so aus:

```
pub   4096R/06ABD620 2015-04-09 [expires: 2017-04-08]
   Key fingerprint = 561C 013A 414D 7DA1 CFCA F074 E630 8682 06AB D620
uid                  Max Mustermann (Musterfirma) max.mustermann
lf:sub   4096R/4126AAC8 2015-04-09 [expires: 2017-04-08]
```

„06ABD620“ stellt in diesem Beispiel die Key-ID in Kurzform dar. Nach der Erstellung des Schlüssels wird er gehärtet, das heißt, man hinterlegt in den Metainformationen, dass bevorzugt die stärksten Algorithmen zum Einsatz kommen sollen. Für die Erstellung eines Firmenschlüssels trägt man statt dem Namen einer Person den kompletten Firmennamen ein und lässt die Angabe einer persönlichen E-Mail-Adresse weg. Falls man eine zentrale allgemeine E-Mail-Adresse für Fragen zum Firmenschlüssel einrichten möchte, kann man diese jedoch gerne angeben.

```
> gpg --edit-key 0x06ABD620
gpg> setpref SHA512 SHA384 SHA256 SHA224 AES256 AES192 AES CAST5 ZLIB BZIP2 ZIP
Uncompressed
gpg> save
```

Anschließend wird, in der Regel mithilfe des separaten Hauptschlüssels, ein Unterschlüssel zum Signieren erzeugt.

```
> gpg --edit-key 0x06ABD620
gpg> addkey
Please select what kind of key you want:
(3) DSA (sign only)
(4) RSA (sign only)
(5) Elgamal (encrypt only)
(6) RSA (encrypt only)
Your selection? 4
[...]
gpg> save
```

Nun kann man noch eine weitere User-ID einfügen, in der keine E-Mail-Adresse genannt wird. Falls der öffentliche Schlüssel auf einem Schlüsselserver hinterlegt werden soll, kann das bei der Vermeidung von Spam recht nützlich sein.

```
> gpg --edit-key 0x06ABD620
gpg> adduid
Real name: Max Mustermann
Email address:
Comment: Musterfirma
You selected this USER-ID:
    "Max Mustermann (Musterfirma)"

Change (N)ame, (C)omment, (E)mail or (O)kay/(Q)uit? o

pub  4096R/06ABD620  created: 2015-04-09  expires: 2017-04-08  usage: SC
           trust: ultimate   validity: ultimate
sub  4096R/4126AAC8  created: 2015-04-09  expires: 2017-04-08  usage: E
sub 4096R/B5229432 created: 2015-04-09 expires: 2017-04-08 usage: S
[ultimate] (1)  Max Mustermann (Musterfirma) max.mustermann
lf:[ unknown] (2). Max Mustermann (Musterfirma)

gpg> uid 2
gpg> primary
gpg> save
```

Zum guten Schluss muss der Schlüssel noch aufgeteilt werden, damit man die Unterschlüssel an die Mitarbeiter ausgeben kann.

```
> gpg --export 0x06ABD620 > archive/max.mustermann/ 7
                                          gpgkey_0x06ABD620.public.gpg
> gpg --export-secret-keys 0x06ABD620 >
archive/max.mustermann/gpgkey_0x06ABD620.secret.gpg
> gpg --export-secret-subkeys 0x06ABD620 >
archive/max.mustermann/gpgkey_0x06ABD620.secret.subkeys.gpg
```

Jetzt sind alle Aktionen am Schlüssel durchgeführt und er ist ins Archiv exportiert. Die Datei gpgkey_0x06ABD620.secret.subkeys.gpg geht an den Mitarbeiter Max Mustermann, die Datei gpgkey_0x06ABD620.secret.gpg bleibt im Archiv, um bestehende Unterschlüssel oder User-IDs zurückzuziehen oder neue zu erzeugen. Der Public Key kann nun an Kommunikationspartner verteilt werden, beispielsweise auf einem firmeneigenen Keyserver. Ansonsten wird er anderweitig in der Firma verteilt, sodass auch alle Mitarbeiter untereinander verschlüsselt kommunizieren können, was bei der flächendeckenden Einführung im Unternehmen immens hilfreich ist. Falls das Unternehmen eine Verschlüsselungslösung einsetzt, die nur mit einem bestimmten Keyserver verkehrt, kann man so auch exakt festlegen, welche öffentlichen Schlüssel Verwendung finden dürfen. Für die Übermittlung der Schlüsselpaare an den Mitarbeiter eignet sich z.B. ein automatisch verbundenes Netzlaufwerk, auf das nur der betreffende Anwender Zugriff hat. Eine manuelle Verteilung über Datenträger ist natürlich ebenfalls denkbar.

Private Schlüssel der Mitarbeiter können in die Hände von Unbefugten geraten, die dann die Kommunikation mitlesen oder falsche Informationen durch eine Signatur als echt erscheinen lassen. Beim Ausscheiden eines Mitarbeiters sollte sein öffentlicher Schlüssel nicht mehr verwendet werden. In diesen Fällen lässt sich ein Schlüssel mit einem Widerrufszertifikat zurückziehen. Alternativ kann man auch nur Teile eines Schlüssels zurückzuziehen. Dies erfolgt jedoch nicht über ein Rückzugszertifikat, sondern über eine spezielle Zertifizierung des Hauptschlüssels. Der entsprechende private Schlüssel bzw. die Schlüsselkomponente kann dann keine Daten mehr signieren, und der öffentliche Schlüssel kann nicht mehr zur Verschlüsselung verwendet werden. Das Entschlüsseln von Daten bleibt jedoch weiterhin möglich.

Ohne einen Offline-Hauptschlüssel muss das gesamte Schlüsselpaar widerrufen werden. Bekommt der Mitarbeiter danach ein neues Schlüsselpaar, muss er sich dieses wieder von allen Kommunikationspartnern signieren lassen. Falls den Mitarbeitern nur ein Unterschlüssel ausgegeben wurde, reicht es, genau diesen zu widerrufen. So bleiben zuvor aufgebaute Vertrauensbeziehungen bestehen. Ein als unbrauchbar markierter öffentlicher Schlüssel sollte zeitnah an alle Kommunikationspartner verteilt werden. Idealerweise kommuniziert man hierbei auch den neuen Schlüssel und aktualisiert vorhandene Schlüsselserver.

Rechteverwaltung regeln

Ein oft vernachlässigtes Thema ist die Festlegung und Durchsetzung von generellen Richtlinien zum Umgang mit Schlüsseln innerhalb des Unternehmens. Falls es die Verschlüsselungssoftware ermöglicht, kann der Administrator einzelnen Benutzern und Gruppen ganz gezielt bestimmte Rechte entziehen oder erteilen. Richtlinien ersparen einerseits viel Arbeit in der täglichen Verwendung, zum anderen verhindert etwa ein Untersagen des Hochladens öffentlicher Schlüssel, dass der „soziale Graph“ der Vertrauensbeziehungen eines Anwenders öffentlich einsehbar wird – und sich somit (falsche) Rückschlüsse auf Unternehmensstrategien ziehen lassen.

Ein häufiger Einwand gegen den Einsatz von E-Mail-Verschlüsselung besagt, dass verschlüsselte Nachrichten in Archiven nicht ohne Weiteres gelesen werden können. Das ist in der Tat richtig, aber bei verschlüsselter Kommunikation auch so erwünscht. Auditoren von E-Mail-Archiven kann jedoch der Zugriff auf das archivierte Schlüsselmaterial gewährt werden. Dazu sollten am besten schon während der Planung entsprechende Zugriffsrechte festgelegt werden.

Bisweilen wächst die E-Mail-Verschlüsselung sukzessive ins Unternehmen hinein, da einzelne Mitarbeiter mit oder ohne Billigung der Unternehmensleitung bereits mit selbst erstelltem Schlüsselmaterial arbeiten.

Aus unternehmerischer Sicht kann man es aber nicht gutheißen, wenn ein Zugriff auf verschlüsselte Nachrichten nur in Kooperation mit dem jeweiligen Schlüsselinhaber möglich ist. Bei Urlaub und Krankheit oder auch beim Ausscheiden des Mitarbeiters aus dem Unternehmen geht so womöglich der Zugriff auf wichtige Informationen verloren. Solche Schlüssel sollte man samt einer funktionierenden Passphrase einsammeln und sicher archivieren. Durch das Zurückziehen alter und die Verteilung neuer Schlüssel lässt sich die Situation aber im Sinne des Unternehmens bereinigen.

Fazit

Erfreulicherweise hält sich der Aufwand bei der Einführung von E-Mail-Verschlüsselung mit OpenPGP in Grenzen. Auch umfangreiche Investitionen sind nicht zwingend erforderlich. Allerdings müssen die Arbeitsabläufe definiert und mit den Mitarbeitern kommuniziert werden, damit die neu gewonnene Sicherheit nicht gleich wieder zunichtegemacht wird. Gleichzeitig soll aber auch die Akzeptanz nicht darunter leiden. Hier bedarf es also einer sorgfältigen Planung – egal ob OpenPGP-basierte Lösungen im Unternehmen bereits vorhanden sind oder erst ausgerollt werden sollen.

Hans-Joachim Giegerich
Geschäftsführer Giegerich & Partner

Digitale Vernetzung im Gesundheitswesen

Der Masterplan für eine zukunftssichere E-Health-Infrastruktur scheint zu stehen

Die Planungen für die elektronische Gesundheitskarte und eine passende telematische Infrastruktur in Deutschland wurden intensiv diskutiert. Der Informationsstand ist aber sogar in Fachkreisen oft dürftig und von Pseudodebatten geprägt. Dabei ist das konzeptionell solide Projekt recht visionär aufgesetzt.

Das gesamte deutsche Gesundheitswesen soll zukünftig mittels einer dedizierten Telematikinfrastruktur (TI) sicher und sektorenübergreifend, etwa zwischen ambulantem und stationärem Bereich, digital vernetzt werden. Elektronik ersetzt Papier. Das ist eine Infrastrukturmaßnahme von einschneidender Bedeutung für jeden Bürger. Diese Kurzübersicht will etwas Transparenz in die Details des Megaprojekts bringen. Dafür lohnt sich zunächst ein Blick auf die vier Kernkomponenten der anvisierten Telematikinfrastruktur: Gesundheitskarten, Heilberufsausweise, Konnektoren und gesicherte Vernetzung.

Physische Zugangsarten

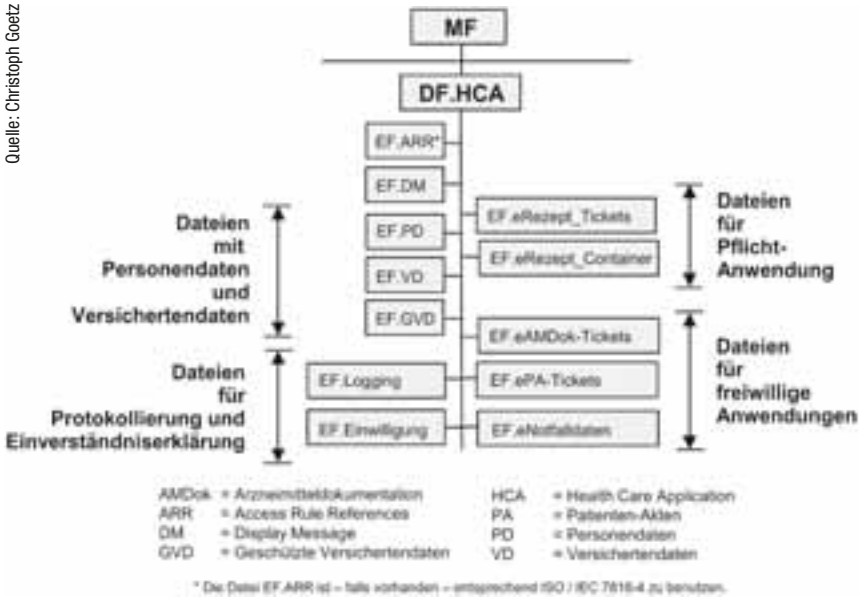
Die neue *elektronische Gesundheitskarte* (eGK) dient für jede gesetzlich versicherte Person in Deutschland als Versicherungsnachweis und gewährt Zugang zu den Leistungen der Gesetzlichen Krankenversicherung (GKV). Physisch ist sie eine Mikroprozessorkarte mit zertifiziertem Kartenbetriebssystem (COS). Sie trägt die Sicherheitsprüfung des Bundesamtes für Sicherheit in der Informationstechnik (BSI) auf der Stufe „Hoch“ mit Kopier- und Änderungsschutz sowie PIN-Funktionen für die Zugriffe. Das COS unterstützt hochwertige Kryptografie und unterbindet jeden Zugriff auf die im Chip gespeicherten Schlüssel. Beim Rollout enthält sie im Wesentlichen die gleichen Stammdaten wie die bisherige Krankenversichertenkarte (KVK), also Name, Anschrift, Versicherungsverhältnis usw., das Ganze jedoch zweimal (einmal im alten KVK-Stil und einmal in einem gesicherten Container, also vergleichbar einer signierten Datei). Darüber hinaus trägt sie ein Bild des Versicherten und die Braille-Kennzeichnung „eGK“. Die Datenfelder im Chip enthalten Zertifikate mit zwei Schlüsselpaaren: eines für die Anmeldung (also Authentifizierung) und eines für die Ver- und Entschlüsselung. Weitere Container im Chip sind definiert und können später je nach PIN-Freischaltung gelesen, geschrieben oder aktualisiert werden. Zusätzlich enthalten die Karten ein Card Verifiable Certificate zur Abwicklung von Card-to-Card-Mechanismen. Ein CV-Zertifikat kann direkt von einer Chipkarte gelesen und direkt durch eine andere Karte verifiziert werden.

Spezielle *Heilberufsausweise* (HBA) gibt es für die Mitglieder der vier verkammerten Heilberufe, also die Ärzte, Zahnärzte, Apotheker und Psychotherapeuten. Auch sie sind Chip-Karten mit geprüftem und zertifiziertem COS. Sie enthalten mittels Postident und Kammerbestätigung verifizierte Stammdaten und tragen ein Bild des Heilberuflers. Die Datenfelder im Chip enthalten HBA-Attribute, Signaturen und Zertifikate mit drei Schlüsselpaaren: eines für die Anmeldung, eines für die Ver- und Entschlüsselung und ein drittes für die Qualifizierte Elektronische Signatur (QES) nach dem deutschen Signaturgesetz. Auch diese Karten enthalten ein CV-Zertifikat. Sie ersetzen die bisherigen Kammerausweise aus Karton oder in Leporelloform.

Neue Netzstrukturen

Neben den speziellen (Dual-Slot-)E-Health-Kartenterminals, die zum Stecken, Auslesen und zur gegenseitigen Authentifizierung der eGK und HBA zum Einsatz kommen und ebenfalls zum Schreiben und zur Aktualisierung der Gesundheitskarten verwendet werden, ist der *Konnektor* eine der wichtigsten dezentralen Komponenten der TI. Er sitzt

Quelle: Christoph Goetz



Die Elementary Files (EF) der eGK decken alle relevanten Bereiche ab.

zwischen dem Praxis- oder Kliniknetz und dem Wide Area Network der TI. Netzwerktechnisch bildet er das Bindeglied zwischen den Primärsystemen, also Praxis oder Klinik, und den Diensten und Anwendungen der zentralen TI der Leistungserbringer. Er verfügt mittels Security Module Card (SMC) über eine eigene elektronische Identität und funktioniert gleichzeitig als Netz- und Anwendungskonnektor sowie als Signaturanwendungskomponente. Die Anwendungen laufen dabei nach einem serviceorientierten Architekturansatz (SOA) ab. Sie werden lastverteilt und bestimmte Nachrichtentypen werden durch das Ersetzen von personenbezogenen Zertifikaten (durch Rollenzertifikate) anonymisiert.

Konzeptionell und funktionell eng mit dem Konnektor verbunden ist die Architekturentscheidung, grundsätzlich nur *gesicherte Vernetzung* mittels Tunnel, als sogenannte Virtuelle Private Netze (VPNs), zuzulassen. Der Konnektor baut IPsec-Tunnel zu den VPN-Zugangsdiensten auf, die aus den verschiedenen Netzwerken der Leistungserbringer angeboten werden. Das ermöglicht eine dezentrale Nutzung von zentralen und fachanwendungsspezifischen Diensten vieler verschiedener Anbieter sowie die Auswahl von Anwendungsoptionen für die Nutzung eines speziell gehärteten Internetzugangs.

Erweiterte Sicherheitskomponenten

Es gibt aber noch andere wichtige Authentifizierungskomponenten für die geplante TI und noch weitere Akteure. Langfristiges Ziel ist eine gemeinsame, zuverlässige und sichere Vernetzung für das gesamte deutsche Gesundheitswesen mit vergleichbarer Qualität für alle Beteiligten. Anforderungen auf gleicher Augenhöhe sind in der TI des Gesundheitswesens besonders wichtig. Jedes Sicherheitsprinzip würde zusammenbrechen, wenn sich z.B. die Heilberufsangehörigen durch qualifiziertes „Haben und Wissen“ (also Karte und PIN) ausweisen müssten, während sich andere Gesundheitsakteure nur mit Namen und Passwort (also nur „Wissen“) oder einfach ungesichert einklinken könnten. Die Entwickler haben das erkannt, entsprechende Lösungsansätze sind weit fortgeschritten, teilweise schon in Erprobung.

Rein technisch betrachtet werden neben den Heilberufsausweisen, die auf eine individuelle Person ausgestellt sind, auch elektronische Sicherungs- und Identitätsobjektanker für andere Zuschnitte bzw. Kollektive benötigt:

Die *gSMC-KT* (gerätespezifische Security Module Card für Kartenterminals) implementiert durch ein eingebautes Sicherheitsmodul die Identität des E-Health-Kartenterminals. Sie dient der sicheren Kommunikation mit anderen Komponenten der TI (z.B. durch Unterstützung einer Remote-PIN-Eingabe).

Die *gSMC-K* (gerätespezifische Security Module Card für Konnektoren) implementiert, ebenfalls durch ein eingebautes Sicherheitsmodul, die Identität des Konnektors. Auch sie sorgt für eine sichere Kommunikation innerhalb der TI.

Die *SMC-B* (Security Module Card, Type B) dient der Authentisierung und elektronischen Signatur für Organisationen des Gesundheitswesens. Sie ist also nicht auf eine einzelne Person, sondern auf eine ganze Abteilung oder Praxis ausgerichtet.

Das *HSM-B* (Hardware Security Module, Type B) kann die kryptografischen Aufgaben einer SMC-B für große Organisationen des Gesundheitswesens, wie z.B. ganze Krankenhäuser, übernehmen, falls die Performance der einfachen SMC-B nicht ausreicht.

Zugangskontrolle für freie Heilberufe

Ein anderer Blickwinkel richtet sich auf jene Heilberufsgruppen, die nicht in Kammern organisiert sind, aber ebenfalls Zugriff auf die TI des Gesundheitswesens benötigen bzw. darüber angesprochen werden müssen. Für sie wurde ein für Deutschland ganz neues elektronisches Gesundheitsberuferegister (eGBR) gegründet. Es übernimmt die sichere Identifizierung der Antragsstellenden für elektronische Heilberufs- oder Berufsausweise (eHBA/eBA) und überprüft die Berufserlaubnisse in Zusammenarbeit mit den zuständigen Länderbehörden.

Mehr als 30 verschiedene Gruppierungen sind gegenwärtig im eGBR vertreten, darunter der Arbeitgeber- und BerufsVerband Privater Pflege e.V. (ABVP), der Bund freiberuflicher Hebammen Deutschlands e.V. (BfHD), die Bundesinnung der Hörgeräteakustiker (BIHA), der Bundesinnungsverband für Orthopädie-Technik (BIV-OT) und der Bundesverband für Ergotherapeuten in Deutschland e.V. (BED).

Schutz persönlicher Daten

Die Vertrauenswürdigkeit jeder TI hängt in starkem Maße davon ab, wie wirksam und konsequent geplante Sicherheitsmaßnahmen konkret umgesetzt werden. Für das deutsche Gesundheitswesen ist der Sicherstellungsauftrag nach dem Zwei-Schlüssel-Prinzip formuliert und auf der Basis von eGKs und HBAs gewissermaßen in Silizium verankert. Die Technik hat entsprechend robuste Mechanismen für die gegenseitige Authentifizierung umgesetzt.

Das Zwei-Schlüssel-Prinzip zwischen den beiden Karten stellt sicher, dass der Zugriff auf medizinische Daten der eGK immer den gleichzei-

tigen Einsatz der eGK und eines HBA erfordert. Erst wenn die eGK durch eine erfolgreiche Card-to-Card-Authentisierung festgestellt hat, dass sie sich einem gültigen HBA im erhöhten Sicherheitszustand (also nach PIN-Eingabe) gegenübersieht und auch der Versicherte seine PIN eingegeben hat, ist der Zugriff auf die medizinischen Datencontainer oder die Nutzung des geheimen Schlüsselmaterials auf der eGK möglich.

Auf ausdrücklichen Wunsch des Versicherten können über die obligaten Stammdaten hinaus medizinische Informationen freiwillig in den Containern verschlüsselt und PIN-geschützt auf der Karte gespeichert werden. Wegen des begrenzten sicheren Speichers der Karten steht dafür nur ein bestimmter Anteil des Datenvolumens zur Verfügung. Entsprechende Kartenmechanismen (Containermodelle) gibt es schon, doch die Sachdiskussion über konkrete Anwendungen ist noch nicht abgeschlossen. Geplant sind verschiedene Datencontainer, z.B. zur Prüfung der Arzneimitteltherapiesicherheit, ein elektronisches Patientenfach oder eine elektronische Patientenquittung. Bei großen Datenvolumen, etwa für elektronische Patientenakten oder CT-Bilder, wären aber auch indirekte Verweise nach dem Pointer-Schlüssel-Prinzip möglich. In jedem Fall bleibt der Versicherte immer Herr über diese Daten. Er kann sie seinem Arzt zur Verfügung stellen oder eben nicht, sie verstecken oder jederzeit löschen lassen. Implementiert und beweisbar gesichert wird dies immer über das Zwei-Schlüssel-Prinzip.

Sonderfall: Freiwillige Notfallregelungen

Von dieser eisernen Regel gibt es zwei Ausnahmen. Genau genommen handelt es sich um zwei voneinander unabhängige, aber auch vollkommen freiwillige Anwendungen mit einer gleichgelagerten Herausforderung für deren Nutzung: Zum einen geht es um das Erstellen und Pflegen eines Notfalldatensatzes (NFD) und zum anderen um das Anlegen eines Datensatzes Persönliche Erklärungen (DPE).

Der NFD beinhaltet Informationen aus der Vorgeschichte des Patienten, die einem behandelnden Arzt zur Abwendung eines ungünstigen Krankheitsverlaufs möglichst schnell und strukturiert zugänglich sein müssen (z.B. Herzschrittmacherdaten, Informationen zu Nierenersatztherapie oder Allergien usw.). Der NFD ist etwa dann wichtig, wenn ein Patient in die Notaufnahme kommt.

Der DPE ist ein eigenständiger Datensatz unabhängig vom NFD. Er enthält Hinweise auf von Willenserklärungen des Patienten zum Behandlungsverlauf oder zur Organ- und Gewebespende. Dabei sind nicht die persönlichen Erklärungen selbst hinterlegt, sondern nur ein Querverweis auf den Ort, an dem sie aufbewahrt werden.

Bei jenen Versicherten, die diese Anwendungen nutzen möchten, sind beide Datensätze getrennt voneinander auf der eGK abgelegt. Für die Anlage dieser freiwilligen Daten ist eine schriftliche Einwilligung erforderlich. Der Name des Arztes, bei dem die Einwilligung hinterlegt ist, wird in der eGK dokumentiert. Der Versicherte kann seine Einwilligungen jederzeit widerrufen. Durch das Löschen von NFD und/oder DPE wird dann auch die jeweilige Dokumentation der Einwilligung von der eGK entfernt.

Lässt der eGK-Inhaber NFD und/oder DPE als freiwillige Anwendung in seine Karte aufnehmen, gilt für den Zugriff auf diese Datenblöcke ein Sonderfall, da die Mitwirkung des Versicherten im akuten Bedarfsfall ja nicht immer möglich ist. Die beiden Datensätze werden zugriffsgeschützt, jedoch nicht verschlüsselt auf der eGK gespeichert. Wären die Daten verschlüsselt auf der eGK hinterlegt, so würde die Nutzung immer die Eingabe der PIN des Versicherten erfordern. Dies wäre jedoch unvereinbar mit dem Sinn und Zweck der Anwendungen.

Technisch läuft dieser Mechanismus übrigens über das Bit 18 der Flag-Liste im CV-Zertifikat des Heilberufsausweises. Es ist nur bei Ausweisen von Ärzten und deren medizinischen Mitarbeitern sowie bei Rettungsassistenten gesetzt. Die eGK gestattet den Zugriff auf die beiden Anwendungen (und nur auf diese) in Anwesenheit eines HBA mit diesem Flag auch ohne die PIN-Eingabe des Patienten. Die technische Durchsetzung des Zugriffsschutzes erfolgt dabei direkt über das Kartenbetriebssystem der eGK, das den Zugriff erst nach Authentifizierung und Verifizierung des HBA freigibt.

Fazit

Insgesamt ist die Einführung der Vernetzung im deutschen Gesundheitswesen eine Infrastrukturmaßnahme von erheblicher Größe und Komplexität. Allein schon die Eckdaten machen das deutlich: Im Vollausbau ergibt sich durch die Nutzerzahlen von ca. 70 Mio. Versicherten, von über 200.000 Leistungserbringern, von annähernd noch einmal so vielen Institutionen und von einigen weiteren Hunderttausend technischen Komponenten mit einem oder mehreren Zertifikaten eine Verzeichnisinfrastruktur von bisher kaum gekannter Größe. Ungeduld mit der Lösung der nationalen Herausforderungen hieße jedoch ein Kapitulieren vor dieser großen und wichtigen Gesellschaftsaufgabe. Und das hätte Nachteile für jeden von uns – wenn wir einmal selbst gesundheitliche Hilfe in Anspruch nehmen müssen.

Dr. Christoph F-J Goetz
Leiter Gesundheitstelematik
Kassenärztliche Vereinigung Bayerns

Rechtssichere und vertrauliche E-Mail-Kommunikation

Auch kleine und mittlere Unternehmen dürfen die Sicherheit im Datenverkehr nicht vernachlässigen

Die Kommunikation über E-Mail mit Kunden und Geschäftspartnern ist mittlerweile zur Lebensader im Tagesgeschäft vieler Unternehmen und Organisationen geworden. Den meisten Nutzern ist jedoch noch immer nicht bewusst, dass eine unverschlüsselte E-Mail so offen wie eine simple Postkarte ist.

Täglich werden Unmengen geschäftlicher Informationen – darunter auch unternehmenskritische Vorgänge und sensible Daten – über ein Postkartensystem namens E-Mail versendet. Die übermittelten Informationen sind nicht nur prinzipiell für jeden lesbar, sie können auf dem Transportweg auch manipuliert oder sogar komplett gelöscht werden. Hinzu kommt ein weiterer Aspekt, der gerade beim Austausch von rechtsrelevanten Dokumenten (z.B. Rechnungen oder Lastschriftmandaten) wichtig ist: Wie kann ich sicher sein, mit wem ich kommuniziere?

Warum verschlüsseln?

Jeder verantwortungsbewusste Nutzer sollte sich fünf zentrale Fragen zu seiner E-Mail-Kommunikation stellen: Benötige ich eine verbindliche Bestätigung der Zustellung? Möchte ich Rechtsgeschäfte per E-Mail abwickeln? Muss ich die Authentizität des Absenders sicherstellen? Muss ich Inhalte vor einer Manipulation sichern? Und: Welcher Schaden kann entstehen, wenn die Informationen und Daten in die Hände Dritter gelangen?

Vor allem zwei Motivationen bringen Entscheider schließlich dazu, sich mit dem Thema Verschlüsselung zu beschäftigen. Zum einen gibt es das ureigene Interesse eines Unternehmens oder einer Organisation, bestimmte Daten wirklich geheim zu halten. Kunden- und Finanzdaten, Konzepte und Informationen über neue Entwicklungen sollen zum Schutz vor Industriespionage und Manipulation verschlüsselt werden. Zum anderen gilt es, die Compliance zu erfüllen. Der Gesetzgeber macht beispielsweise im Bundesdatenschutzgesetz (BSDG) Vorgaben zum Umgang mit personenbezogenen Daten und nimmt die Geschäftsführung persönlich in die Haftung. Die Verschlüsselung von E-Mails stellt einen wesentlichen Schritt hin zu einer vertrauenswürdigen E-Mail-Kommunikation dar. Damit wird aus der gewöhnlichen Postkarte gewissermaßen eine Postkarte mit Geheimschrift, die nur der berechtigte Empfänger lesen kann.

Die Bedrohungslage

Im Rahmen einer Studie von Corporate Trust („Industriespionage 2014 – Cybergeddon der Wirtschaft durch NSA & Co.?“) wurden in Deutschland und Österreich die Risiken von Cyberangriffen samt einiger aktueller Vorfälle erfasst. Die Studie gelangt u.a. zu folgendem Ergebnis: Mehr als die Hälfte (54,3 %) der befragten Unternehmen in Deutschland hatten bereits einen Spionagevorfall oder zumindest den Verdacht, dass ein Angriff stattgefunden habe. Nahezu jedes zweite betroffene Unternehmen (41,1 %) nennt das „Abhören/Abfangen von elektronischer Kommunikation“ als bewiesene oder vermutete Handlung des Angreifers. Aber nur 16 % der Unternehmen nutzen E-Mail-Verschlüsselung als ein zentrales Instrument der IT-Sicherheit.

Die Verschlüsselung der Unternehmenskommunikation, insbesondere über E-Mail, setzt also an einem bekannten Schwachpunkt an. Sie könnte die Schwelle für potenzielle Angreifer deutlich erhöhen. Die notwendigen Technologien und Werkzeuge sind vorhanden, werden aber in der Praxis zu selten oder nicht konsequent genug eingesetzt.

Die Anwendersicht

Eine Erklärung für die geringe Nutzung vorhandener Instrumentarien aus dem Bereich der Mail- und Datenverschlüsselung lässt sich aus den in der Praxis weitverbreiteten Anwendersichten auf das Thema IT-Sicherheit ableiten. Insbesondere in kleinen und mittleren Unternehmen (KMU) begegnen sowohl Entscheider als auch Nutzer den Gefahren und Risiken vernetzter IT-Systeme oft mit zu wenig Sensibilität und Aufmerksamkeit. Der Schutzbedarf der eigenen IT-Systeme und der verarbeiteten und gespeicherten Daten wird erfahrungsgemäß viel zu gering eingeschätzt.

In allen Unternehmen und Organisationen, die IT-Systeme nutzen, muss also dringend das Bewusstsein für die drohenden Gefahren erhöht werden. Entscheider und Anwender sollten in die Lage versetzt werden, den Schutzbedarf der Anwendungen und Daten des eigenen Unternehmens oder der eigenen Organisation richtig zu evaluieren und aus dieser Bewertung wirksame Maßnahmen abzuleiten.

Es kann natürlich nicht Ziel einer unternehmensinternen IT-Sicherheitsstrategie sein, sich gegen die umfangreichen Möglichkeiten eines staatlichen Dienstes zu rüsten. Vielmehr muss die Schwelle für den Missbrauch von Daten und Systemen von innen wie von außen durch technische und organisatorische Maßnahmen möglichst hoch gesetzt werden. Hierin liegt der klare Nutzen des Einsatzes verfügbarer, bezahlbarer und praktikabler Lösungen für die Daten- und insbesondere die E-Mail-Verschlüsselung.

Rechtliche Aspekte

Ob und inwieweit der Einsatz von Verschlüsselungsverfahren bei der E-Mail-Kommunikation für den Versender oder Empfänger verpflich-

tend ist, wurde bislang gesetzlich nicht klar geregelt. Deshalb bleiben entsprechende Sicherungsmaßnahmen weitgehend das Ergebnis individueller Risikobeurteilungen. Daraus sollte jedoch nicht der Schluss gezogen werden, dass tatsächlich keinerlei bindende Pflichten beim Austausch von Informationen per E-Mail bestehen.

Im Rahmen der Vertragsgestaltungsfreiheit können Vertragsparteien Klarheit schaffen. Vertragsklauseln zur E-Mail-Verschlüsselung sollten insbesondere im Blick haben, welche Mitarbeiter oder Unternehmensbereiche verpflichtet werden müssen. Weitere Aspekte betreffen Kategorien von Inhalten bzw. Informationen, einzelne Projekte, Geschäftsbereiche und nicht zuletzt bestimmte externe Kommunikationspartner. Dazu ist es sachdienlich, die Eckpunkte zur technischen Umsetzung klarzustellen und gegebenenfalls für Alternativen zu sorgen. Je nach Fall kann es auch opportun sein, Sanktionen für Pflichtverstöße vorzusehen.

Gesetzliche Pflichten und Haftungsrisiken

Ein umfassendes Gesetz zur IT-Sicherheit gibt es bislang nicht. Eine allgemeine Verschlüsselungspflicht gibt es ebenfalls nicht. Vielmehr lassen sich aus unterschiedlichen Normen Maßstäbe für eine E-Mail-Verschlüsselung ableiten, die allerdings nur auf bestimmte Personengruppen (z.B. Ärzte und Rechtsanwälte, § 203 StGB), Branchen und Bereiche sowie auf bestimmte Inhalte Anwendung finden (z.B. personenbezogene Daten, § 9 BDSG). Daneben existieren zwar anerkannte Regelungen, wie z.B. der BSI-Grundschutz, technische Richtlinien oder Branchenstandards. Diese entfalten aber nur bedingt eine Bindungswirkung, da es ihnen an der Allgemeinverbindlichkeit eines Gesetzes fehlt. Dennoch können derartige Standards von einem Gericht herangezogen werden, um im Einzelfall den Sorgfaltsmaßstab zu bestimmen. Es erscheint daher durchaus empfehlenswert, sich mit diesen Standards auseinanderzusetzen.

Verstöße gegen eine Verschlüsselungspflicht können nämlich auch Unterlassungs- und Schadenersatzansprüche gegen das versendende Unternehmen begründen. Dies ist auch für den Fall möglich, dass eine Pflicht zur E-Mail-Verschlüsselung vertraglich nicht ausdrücklich bestimmt wird, es aber eine entsprechende nebenvertragliche Vereinbarung gibt. Darüber hinaus sind Regressansprüche des ersatzpflichtigen Unternehmens gegen die Unternehmensleitung denkbar. Denn die E-Mail-Verschlüsselung gehört als Maßnahme der IT-Sicherheit zum Risikomanagement, für deren Durchführung Geschäftsführer und Vorstände persönlich haften (§ 43 GmbHG, §§ 91, 93, 116 AktG).

Vorhandene Technologien

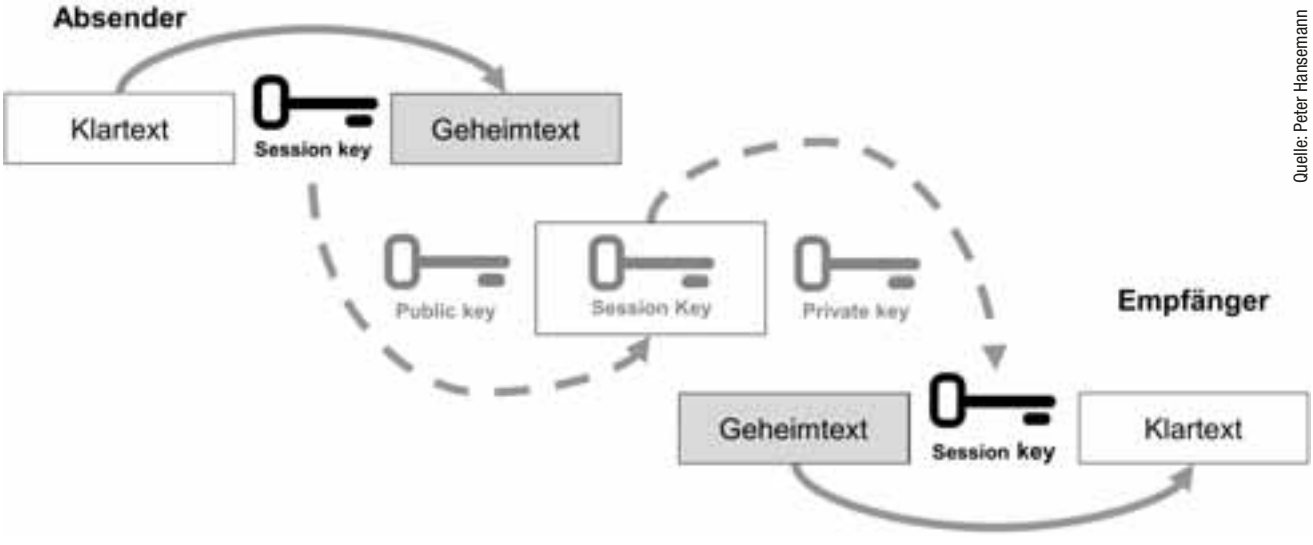
Marktübliche Verschlüsselungsprodukte setzen auf bekannte Algorithmen. Um den Klartext in einen Geheimtext umzuwandeln, wird als Parameter ein Schlüssel benötigt und der stellt das eigentliche Geheimnis dar. Algorithmen wie AES (Advanced Encryption Standard) gelten als sehr sicher. Der Aufwand einer Brute Force Attack, bei der alle möglichen Kombinationen durchgerechnet und ausprobiert werden, steigt mit der Schlüssellänge exponentiell.

Generell unterscheidet man zwischen symmetrischer und asymmetrischer Verschlüsselung. Bei der symmetrischen Verschlüsselung, etwa nach dem AES-Standard, wird derselbe Schlüssel zum Ver- und Entschlüsseln der Daten genutzt. Die Sicherheit ist dabei an die Geheimhaltung dieses Schlüssels gebunden. In der direkten Nutzung zur Kommunikation gibt es das Problem, dass mindestens zwei Parteien diesen Schlüssel zuerst miteinander teilen und ihn anschließend sicher verwahren müssen.

Private und öffentliche Schlüssel

Mit einer Aufteilung in private und öffentliche Schlüssel lässt sich dieses grundsätzliche Problem der Schlüsselverteilung und Geheimhaltung lösen. Nur der private Schlüssel bleibt geheim. Der öffentliche Schlüssel ist kein Geheimnis. Er kann wie eine Telefonnummer von jedermann gefunden und gewählt werden. Nur der Inhaber des privaten Schlüssels ist dann unter dieser Nummer erreichbar.

Asymmetrische Schlüsselpaare werden Identitäten zugeordnet. Hierin begründet sich das Modell der Public-Key-Infrastrukturen (PKIs), die Basis der Public-Key-Kryptografie, welche letztlich die sichere Kommunikation innerhalb unsicherer Netzwerke erlaubt. Die öffentlichen Schlüssel werden als Zertifikate auf bestimmte Identitäten ausgestellt und breit gestreut. Mittels einer Echtheits- und Gültigkeitsprüfung von Zertifikaten können Identitäten zu einem bestimmten Zeitpunkt zweifelsfrei festgestellt werden. PKIs werden im Bereich der E-Mail-Verschlüsselung genutzt, indem Nachrichten mit den Zertifikaten der jeweiligen Empfänger chiffriert werden. Nur der Inhaber des



Quelle: Peter Hansemann

Eine hybride Verschlüsselung kombiniert symmetrische und asymmetrische Verschlüsselungsverfahren (Abb. 1).

privaten Schlüssels zum jeweiligen Zertifikat kann die Nachrichten entschlüsseln.

Zur PKI-basierten E-Mail-Verschlüsselung haben sich zwei Standards etabliert: S/MIME (Secure/Multipurpose Internet Mail Extensions) und OpenPGP (Pretty Good Privacy). Beide nutzen im Grunde die gleichen kryptografischen Verfahren. Sie unterscheiden sich jedoch in der Zertifizierung der öffentlichen Schlüssel und damit in den Vertrauensmodellen. Beide Standards sind nicht zueinander kompatibel, das heißt, Anwender des einen Verfahrens können keine signierten oder verschlüsselten Nachrichten mit Anwendern des anderen Verfahrens austauschen.

Hybride Verschlüsselung

Die Verschlüsselungssoftware generiert zunächst einen symmetrischen Session-Key. Mit diesem werden die im Klartext vorliegenden Daten verschlüsselt. Der Session-Key wird dann mit dem Zertifikat vom Empfänger verschlüsselt und an die Nachricht angehängt. Die verschlüsselte Nachricht enthält nun die Information, mit welchem Zertifikat sie verschlüsselt wurde, damit die Software des Empfängers den zum Zertifikat gehörigen privaten Schlüssel nutzen kann. Der Empfänger erhält die Nachricht. Mit seinem privaten Schlüssel kann er zunächst den symmetrischen Session-Key entschlüsseln, den das Programm des Absenders für diese Nachricht erstellt hat. Mithilfe dieses Session-Keys entschlüsselt die Software des Empfängers schließlich die Originalnachricht (Abbildung 1).

Transportverschlüsselung

Ein wesentlicher Vorteil der Ende-zu-Ende-Verschlüsselung von E-Mails besteht darin, dass kein System auf dem Übertragungsweg auf die Inhalte der E-Mail zugreifen kann. Das bedeutet allerdings gleichzeitig den Verzicht auf Contentfilter, Antivirus, Antispam, Data Loss Prevention und Archivierung. Eine Alternative hierzu bietet die Transportverschlüsselung. Dabei werden die Einzelnachrichten innerhalb eines verschlüsselten Transportkanals (Tunnel) versendet, sodass ein Angreifer weder den Transport abhören noch die übertragenen Daten mitlesen kann. Im E-Mail-Verkehr ist deshalb generell der Einsatz von TLS (Transport Layer Security) oder eines verschlüsselten VPN (Virtual Private Network) mittels IPsec (Internet Protocol Security) für die Übermittlung anzuraten.

Praxislösungen

Idealerweise nutzen E-Mail-Systeme untereinander automatisierte Verfahren für eine sichere Übertragung. In diesem Fall muss der Nutzer sich nicht um die Verschlüsselung kümmern, sondern die betroffenen Serversysteme regeln die Kommunikation untereinander. Obwohl heute erst die wenigsten E-Mail-Server mit den notwendigen Voraussetzungen (Gateway und Zertifikate) ausgestattet sind, ist davon auszugehen, dass sich diese Art der Verschlüsselung insbesondere im Unternehmensbereich durchsetzen wird.

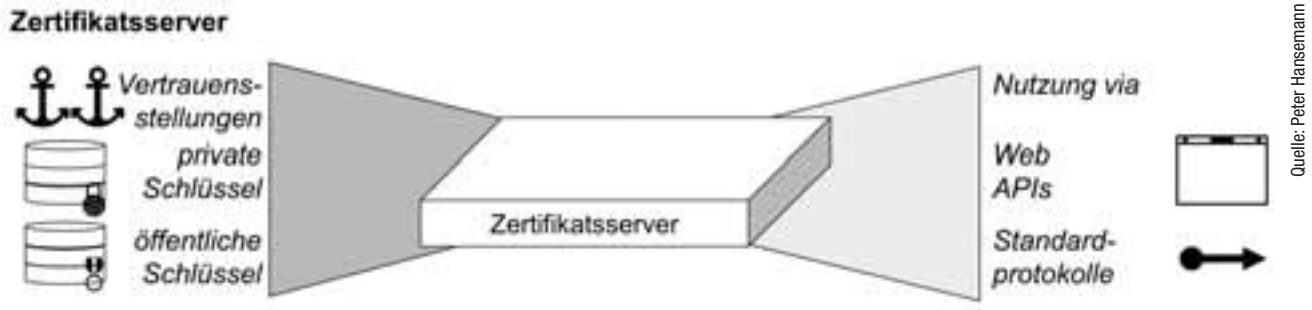
Eine durchgängige Verschlüsselung vom E-Mail-Client des Absenders bis zu demjenigen des Empfängers setzt immer eine vorherige Abstimmung der Kommunikationspartner über die Art der Verschlüsselung sowie den Austausch von Zertifikaten und Schlüsseln voraus. Entsprechend etabliert sich im breiten Unternehmenseinsatz zunehmend die sogenannte Organisations-Ende-zu-Ende-Verschlüsselung (Organizational End-to-End Encryption). Die Verschlüsselung zwischen Unternehmen wird dabei durch E-Mail-Gateways realisiert. Die Nachrichten bleiben so auf ihrem Weg durch das Internet konstant gesichert. Nur beim Absenden bzw. Empfangen im Unternehmen können zentrale Mail-Contentfilter die unabdingbaren Checks auf Viren, Trojaner etc. durchführen.

In heutigen Messaging-Systemen – damit sind sowohl E-Mail-Programme für Endgeräte als auch E-Mail-Serversysteme auf verschiedenen Systemplattformen gemeint – sind standardmäßig Verschlüsselungstechnologien implementiert. Für die Verschlüsselung der Kommunikation zwischen Serversystemen bieten viele auf dem Markt angebotene Produkte beispielsweise die Option an, das Sicherheitsprotokoll TLS zu nutzen. Auch die meisten E-Mail-Clients können Nachrichten mit E-Mail-Servern auf Basis einer verschlüsselten Verbindung austauschen. Diese Mechanismen funktionieren in der Regel auch mit den heute gängigen Freemail-Systemen, die häufig im privaten Bereich zum Einsatz kommen. Somit ließe sich zumindest ein Teil des Übertragungsweges absichern. Leider werden die vorhandenen Möglichkeiten viel zu oft weder von Anwendern noch von Administratoren berücksichtigt.

Zertifikats- und Schlüsselmanagement

Dass die vertrauliche Kommunikation zwischen Absender und Empfänger so einfach wie beschrieben funktioniert, ist natürlich der Idealfall. Es bleibt unabdingbar, dass der Absender das Zertifikat des Empfängers erhält. Vorab sind deshalb bei jeder einzelnen Verschlüsselung folgende Fragen zu klären: Woher bekommt der Absender das Zertifikat des Empfängers? Ist es echt und ist es gültig?

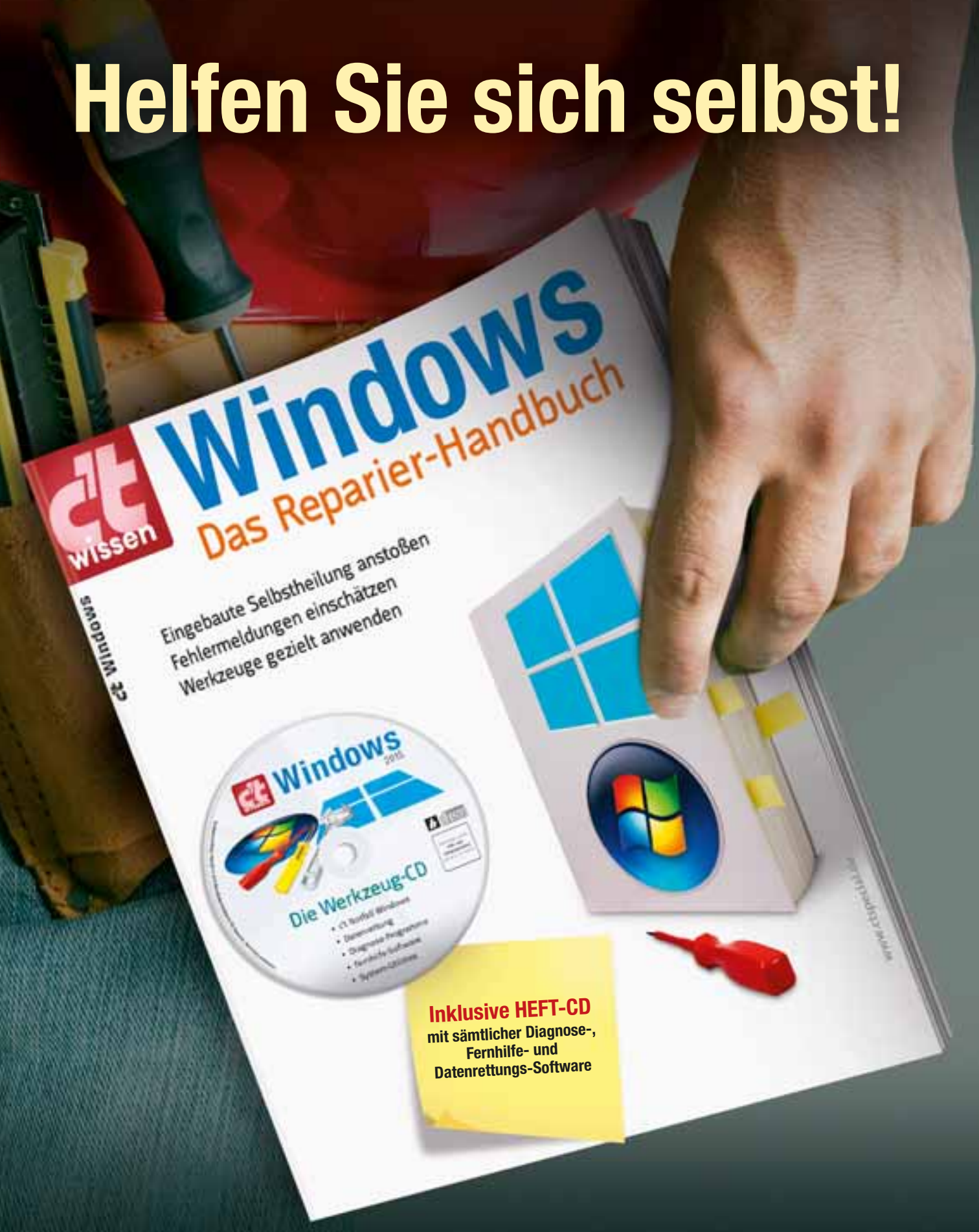
Die Komplexität der PKI mit der Fülle an Informationen zur Echtheits- und Gültigkeitsprüfung macht ein manuelles Schlüssel- und Zertifikatsmanagement praktisch unmöglich. Dafür sind Lösungen entwickelt worden, die als Zertifikatsserver bezeichnet werden. Sie übernehmen automatisiert das Management der Zertifikate und öffentlichen Schlüssel einschließlich deren Verifizierung und Validierung (Abbildung 2).



Quelle: Peter Hansemann

Externe Server stellen Schlüssel und Zertifikate abgesichert im Internet bereit (Abb. 2).

Helfen Sie sich selbst!



Bestellen Sie Ihr Exemplar für 8,40 €*:

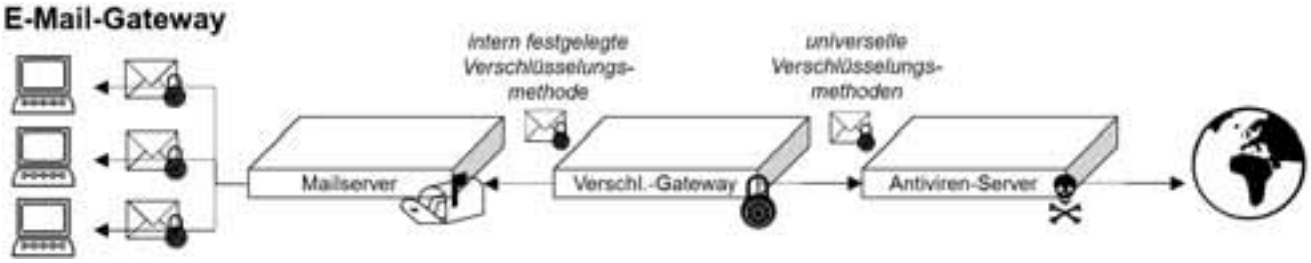
shop.heise.de/ct-windows-2015 service@shop.heise.de

Auch als eMagazin erhältlich unter: shop.heise.de/ct-windows-2015-pdf

* portofreie Lieferung für Heise Medien- oder Maker Media Zeitschriften-Abonnenten oder ab einem Einkaufswert von 15 €

heise shop

shop.heise.de/ct-windows-2015



Quelle: Peter Hansemann

Über ein Gateway lassen sich Nachrichten auf unterschiedliche Weise verschlüsseln (Abb. 3).

Mit der European Bridge CA (EBCA) hat TeleTrusT eine Initiative ins Leben gerufen, die einen komfortablen Austausch verschlüsselter Daten gewährleistet. Sie stellt einen Zusammenschluss einzelner, gleichberechtigter Public-Key-Infrastrukturen zu einem PKI-Verbund dar und ermöglicht die sichere und authentische Kommunikation zwischen den beteiligten Unternehmen, Institutionen und öffentlichen Verwaltungen.

Serverbasierte Lösungen

Im Bereich der E-Mail-Verschlüsselung sind sogenannte Secure E-Mail Gateways weit verbreitet. Diese sichern serverbasiert und damit zentral und transparent für die Nutzer den gesamten durchlaufenden E-Mail-Verkehr gemäß den eingestellten Regelwerken (Policies).

GEPRÜFTE SICHERHEIT „MADE IN GERMANY“

Der Verbund „E-Mail made in Germany“ bietet eine eigene, für neue Teilnehmer offene Lösung zur Absicherung der E-Mail-Kommunikation, die den TLS-Standard an entscheidenden Stellen um zusätzliche Prüfschritte erweitert. Der Verbund erreicht mit seinem Verschlüsselungsstandard derzeit über 50 Mio. private E-Mail-Nutzer und mehr als 3 Mio. gewerbliche Kunden und hat somit hohe praktische Bedeutung.

Neue Teilnehmer auditiert der TÜV Rheinland im Hinblick auf die Umsetzung des vorgegebenen E-Mail-Standards als „geprüfter E-Mail made in Germany Provider“. Im Audit wird überprüft, ob die Daten ausschließlich in deutschen Rechenzentren verarbeitet werden und die organisatorischen und technischen Prozesse auf dem aktuellsten Sicherheitsstand sind. Außerdem werden verwendete Server und kryptografische Algorithmen daraufhin begutachtet, ob sie dem aktuellen, vom BSI als sicher angesehenen Stand entsprechen. Dadurch lässt sich, zusätzlich zur technischen Umsetzung, ein erhöhtes Sicherheits- und Datenschutzniveau der Teilnehmer attestieren.

Der Endnutzer benötigt beim Einsatz von „E-Mail made in Germany“ für die technische Umsetzung auf dem Mailserver lediglich ein E-Mail-Konto bei einem der Verbundpartner. Er selbst muss keine speziellen Installationen oder Einstellungen vornehmen. Durch eine grafische Darstellung der abgesicherten Kommunikation mittels eines grünen Hakens im Webmailer oder Mailclient wird auch dem technisch nicht versierten Nutzer die Verwendung einer sicheren Transportverschlüsselung klar und deutlich signalisiert. Für Unternehmen lässt sich die Teilnahme am Verbund über eine Gateway-Lösung eines der Verbundpartner realisieren.

Im Rahmen der Implementierung und Nutzung solcher Secure E-Mail Gateways gibt es zahlreiche Verfahren zur Verschlüsselung von E-Mails. Dazu gehören Gateway-Produkte, die auf intelligente Weise die interne und externe E-Mail-Verschlüsselung verknüpfen. Somit lassen sich E-Mails nicht nur über das Internet, sondern auch innerhalb der firmeneigenen Netze verschlüsselt übertragen. Andere Produkte bieten Möglichkeiten der Passwort-basierten Kodierung über PDF-Dateien oder ZIP-Container. Darüber hinaus kommen Verfahren wie HTML-Push- bzw. -Pull-Mails (Verschlüsselung der gesamten Nachricht als HTML-Anhang) oder die S/MIME-Verschlüsselung mit Ad-hoc-Zertifikatsgenerierung für Empfänger zum Einsatz. Bei der Identity Based Encryption (IBE) – eine ebenfalls PKI-basierte Variante der E-Mail-Verschlüsselung – werden Schlüsselpaare aus Zeichenketten (z.B. E-Mail-Adressen) errechnet (Abbildung 3).

Plug-ins in E-Mail-Clients

Alternativ zu den erwähnten Gateway-basierten Lösungen ist es auch möglich, die Verschlüsselung bzw. Signierung im E-Mail-Client selbst durchführen zu lassen. Die Verwendung von geeigneten Plug-ins stellt oft einen einfachen, ersten Schritt in die Verschlüsselungswelt dar, insbesondere dann, wenn nur einzelne Personen mit verschlüsselten E-Mails arbeiten sollen. Gegenüber dem Einsatz von Gateways birgt diese Methode Vor- und Nachteile, die individuell je nach Anwendungsfall abgewogen werden müssen. Bei der Auswahl eines geeigneten Plug-ins sollten vor allem eine einfache und problemlose Installation sowie die größtmögliche Usability im Vordergrund stehen. Denn gerade Neuanwender profitieren von einer Benutzerführung, die Fehler vermeiden hilft.

Fazit

Die Zukunft einer rechtssicheren und vertrauenswürdigen E-Mail-Kommunikation, insbesondere zwischen einzelnen Unternehmen und Organisationen, liegt in der verschlüsselten Übertragung. Möglichkeiten wie die PDF-Verschlüsselung oder HTML-Verfahren bieten pragmatische Ansätze für eine zielgerichtete Nutzung und bereiten damit auch für kleine und mittlere Unternehmen einen gangbaren Weg zu einer zeitgemäßen Geschäftskommunikation.

Private Anwender werden sich allerdings weiterhin auf individuelle Softwarelösungen mit hohem Abstimmungsaufwand zwischen den Kommunikationspartnern einstellen müssen, um Ihre E-Mail-Kommunikation gegenüber unbefugtem Zugriff zu schützen. Erst wenn kommerzielle E-Mail-Provider vergleichbare Systeme anbieten, wie sie in der Unternehmenskommunikation genutzt werden, können auch hier komfortable Lösungen entstehen.

Peter Hansemann
Geschäftsführer ICN GmbH + Co. KG

(Un-)Sicherheit im nationalen Alleingang?

Der Entwurf zum IT-Sicherheitsgesetz wirft mehr Fragen auf, als er beantwortet

Im März 2015 fand im Deutschen Bundestag die erste Lesung zum Entwurf des IT-Sicherheitsgesetzes (ITSiG) statt. Er enthält umfängliche Meldepflichten für Betreiber kritischer Infrastrukturen, adressiert aber auch andere Unternehmen. Technische oder organisatorische Maßnahmen sind jedoch nicht direkt vorgesehen.

Zentraler Anknüpfungspunkt des Gesetzesentwurfs ist die Einführung einer Definition kritischer Infrastrukturen (KRITIS) in § 2 Abs. 10 BSIG-E. Der zweigliedrige Begriff benennt zum einen das qualitative Kriterium der Zugehörigkeit zu einem grundsätzlich als kritisch eingestuften Sektor. Zum anderen setzt er die quantitative Sicherheitsrelevanz voraus, dass ein Ausfall erhebliche Konsequenzen für Versorgung und öffentliche Sicherheit hätte. Schon hierin liegt ein Schwachpunkt des Ansatzes, denn diese Definition ist wenig belastbar.

Technische und organisatorische Vorkehrungen

Die Tatbestandsmerkmale nicht bereits im Gesetz konkreter zu fassen und Weiteres einer noch zu schaffenden Rechtsverordnung zu überlassen, ist bereits vielfach kritisiert worden. Während die auferlegten Pflichten zur Schaffung angemessener technischer und organisatorischer Vorkehrungen (TOV) sowie zur Einrichtung einer zentralen Kontaktstelle erst mit einer Übergangsfrist entstehen, gilt die Meldepflicht im Störungsfall unmittelbar. Ein Sanktionsregime sieht das BSIG-E übrigens nicht vor. Das bleibt vor dem Hintergrund der unterstellten Sicherheitsrelevanz unschlüssig.

Bei der Umsetzung der TOV ist der „Stand der Technik“ zu berücksichtigen. Was diese Berücksichtigung beinhaltet und warum der Stand der Technik nicht einzuhalten sein soll, erschließt sich nicht, denn eine Definition für den Begriff fehlt im Entwurf. Die Bestimmung der konkreten TOV nicht dem Gesetz, sondern den Betreibern zu überlassen und die Möglichkeit branchenweit gültiger Standards vorzusehen, erscheint zwar flexibel und erlaubt praxisnahe Maßnahmen. Welche Auswirkung das haben wird, bleibt allerdings abzuwarten.

Bedauerlich ist es jedenfalls, dass kein branchenübergreifender Mindeststandard formuliert wurde. Das, was ohnehin jeder einzuhalten hat, kann auch vor die Klammer gezogen werden. Alternativ könnte der Gesetzgeber kategorische Vorgaben machen, wie etwa im Sinne der Regelungsbereiche zu den technischen und organisatorischen Maßnahmen beim technischen Datenschutz. Die Erfahrungen aus dem Umgang mit diesen Maßnahmekategorien wurden in keiner Weise nutzbar gemacht. Denkbar und wünschenswert wären zumindest gesetzliche Bewertungsmaßstäbe für das Instrumentarium gewesen. Maßgeblich könnten hier die Schadensgeneigtheit der Datenverarbeitung, Unternehmensumsätze, o.Ä. sein. Das vom TeleTrusT – Bundesverband IT-Sicherheit e.V. vorgestellte Modell der Wirkungsklassen bietet beispielsweise eine konkrete Verbindung von definierten Schutzbedarfen und assoziierten Maßnahmen.

Spezialgesetze statt Vereinheitlichung

Der Gesetzesentwurf unternimmt nicht den Versuch, die IT-Sicherheit rechtlich in einem Gesetz zu vereinheitlichen. Soweit bereichsspezifische Pflichten bestehen, bleiben sie erhalten. Doch es werden auch neue geschaffen. So soll etwa das Telemediengesetz geändert werden. Danach verpflichtet § 13 Abs. 7 TMG-E die Anbieter auf zumutbare TOV. Warum ihnen aber bei einem Pflichverstoß ein Bußgeld in Höhe von bis zu EUR 50.000 drohen soll, ist nicht nachvollziehbar.

Auch ein Kleinstunternehmerprivileg, wie es für die KRITIS geplant ist, findet sich im Entwurf für das TMG nicht. Gleichermaßen bedauerlich ist die Streichung einer dem § 100 Abs. 1 TKG entsprechenden Norm aus dem Referentenentwurf vom 18.08.2014.

Ebenso gibt es keinerlei rechtssystematische Ansätze zur Vereinheitlichung zwischen dem ITSiG und dem Datenschutz. Dieser bezieht sich lediglich auf personenbezogene Daten. Daten ohne Personenbezug werden aber stetig seltener. Innerhalb definierter Unternehmensbereiche haben Daten mit und ohne Personenbezug ein einheitliches Schutzniveau. Künftig ist also nicht klar, wie sich die Anforderungen des ITSiG und des Datenschutzrechts zueinander verhalten.

Nationaler Alleingang

Parallel wird auf europäischer Ebene gerade die NIS-Richtlinie verhandelt. Als Grundlage eines nationalen ITSiG stellt die NIS-Richtlinie ein Regelungsregime dar, dessen Anforderungen sich nicht mit denen des deutschen Entwurfs decken werden. Die Folgen sind weiterer Änderungsbedarf des ITSiG sowie Rechtsunsicherheit bei den Unternehmen. Auch aus diesem Grund wäre eine europaweite, idealerweise darüber hinausgehende Abstimmung begrüßenswert, denn die IT-(Un)Sicherheit macht an Landesgrenzen keinen Halt.

Fazit

Fragt man sich, ob wir ein IT-Sicherheitsgesetz brauchen, fällt eine Zustimmung leicht. Ob der Entwurf allerdings den berechtigten Erwartungen gerecht wird, muss bezweifelt werden. Vorsicht ist geboten, wenn der deutsche Gesetzgeber den europäischen Richtliniengeber ohne Not überholt. Warum der Bund mit dem ITSiG die eigenen Behörden nicht zu verpflichten gedenkt, bleibt zu beobachten.

RA Karsten U. Bartels, LL.M.
HK2 Rechtsanwälte

Verschlüsselt an alle und überall

Eine effiziente Verschlüsselungstechnik kann heute die gesamte IT-Infrastruktur im Unternehmen absichern

Fast jedes dritte Unternehmen in Deutschland war laut einer aktuellen Studie in den vergangenen zwei Jahren von konkreten IT-Sicherheitsvorfällen betroffen. Cyberattacken auf das geistige Eigentum sind mittlerweile zu einer existenziellen Bedrohung geworden, die auch vor dem Firmenhandy nicht haltmacht.

Angriffe auf die IT-Kommunikation von Unternehmen werden zunehmend von professionellen Organisationen bis hin zu staatlichen Geheimdiensten durchgeführt. Bedrohungen gehen nicht allein von der viel gescholtenen US-amerikanischen NSA aus, sondern insbesondere auch von Diensten aus Ländern wie China, Russland, Iran u.v.a.m. Und das Ausspähen von Daten findet nicht nur an den Überseekabeln statt – die Angriffe erfolgen mehr und mehr direkt im Unternehmensnetzwerk und betreffen alle vernetzten Systeme und Endgeräte. Wichtige Daten müssen also bereits innerhalb des Unternehmens effektiv vor unautorisiertem Zugriff geschützt werden.

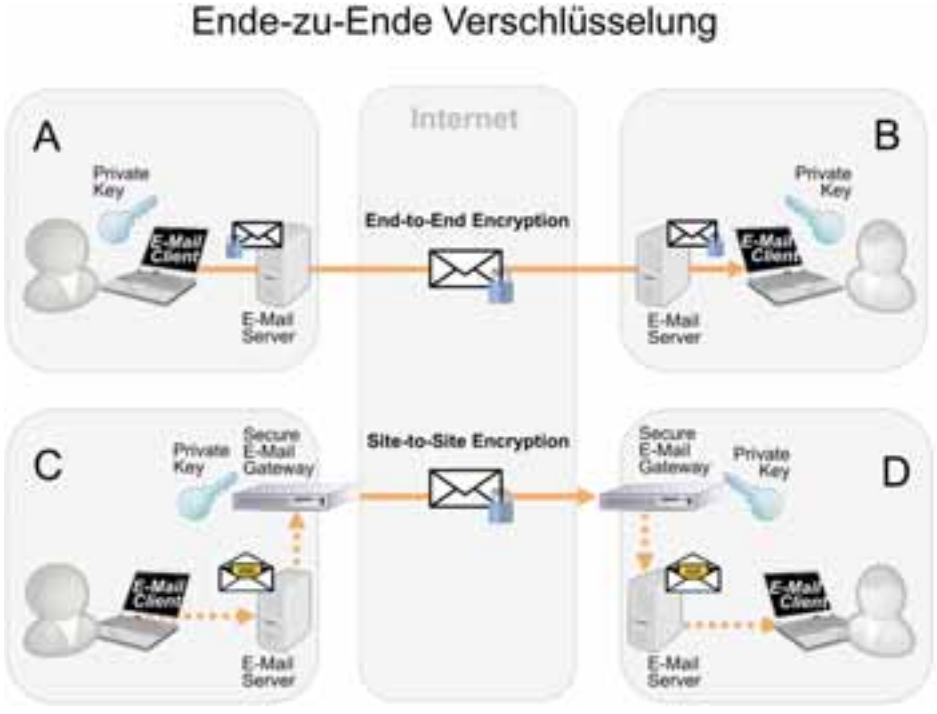
Sicherheit vom Sender bis zum Empfänger

Eine starke Ende-zu-Ende-Verschlüsselung (End-to-End Encryption, kurz: E2EE), die alle Daten bei der Speicherung und der Übertragung wirksam zu schützen vermag, stellt somit schlicht eine wirtschaftliche Notwendigkeit dar. Im Übrigen entspricht eine wirksame Absicherung der Unternehmenskommunikation nicht nur den Anforderungen zur Abwehr von Cyberspionage, sie wird darüber hinaus auch in vielen Bereichen gefordert, um Compliance-Vorgaben oder Datenschutzgesetze zu erfüllen.

Ende-zu-Ende-Verschlüsselung bedeutet, dass eine Nachricht an der Quelle verschlüsselt wird und nicht entschlüsselt werden kann, bis sie am endgültigen Ziel eintrifft. Bereits im E-Mail-Client des Absenders werden die Daten verschlüsselt und erst von der Software des Empfängers wieder entschlüsselt. Eine TLS-Verschlüsselung (Transport Layer Security) zwischen Client und E-Mail-Server bietet übrigens keine echte E2EE, ebenso wenig wie ein Secure E-Mail Gateway. Denn damit sind nur bestimmte Transportstrecken abgesichert. Der Zugriff auf unverschlüsselte E-Mails durch Serverbetreiber oder Administratoren bleibt weiterhin möglich (Abbildung 1).

Was muss verschlüsselt werden?

Wenn man vertrauliche Daten via Internet austauscht, dann kann dies mittels unterschiedlicher Dienste, Protokolle und Datenformate erfolgen. Der klassische Fall ist nach wie vor die E-Mail-Kommunikation. Für den Austausch größerer Dateien eignen sich hingegen Cloud-ba-



Quelle: Gunnar Jacobson

Echte Ende-zu-Ende-Verschlüsselung gewährt Sicherheit auf dem gesamten Übertragungsweg (Abb. 1).

GNADENLOS DURCHLEUCHTET

RADIKAL DIGITAL: DAS PAPIERLOSE c't-ABO

6×c't
NUR 17,70 €

ERLEBEN SIE c't IN DIGITALER QUALITÄT:

- **BEQUEM:** alle 14 Tage freitags in der App
- **2 LESEFORMATE:** im Original-c't-Layout oder interaktiven HTML-Lesemodus
- **VERFÜGBAR FÜR** iOS (iPad, iPhone) und Android (Smartphone, Tablet, Kindle Fire)
- **ZUSÄTZLICHE** Bilder und Videos

UNSER GESCHENK AN SIE:

Eine **15 € Geschenkkarte** für den Google-Play-Store:
Wählen Sie Ihre Lieblingsunterhaltung aus Millionen von Büchern, Songs, Filmen, Apps und vielem mehr aus.

Geschenkkarten von Google-Play sind unbegrenzt haltbar und im Web sowie auf jedem Android-Gerät einlösbar.

JETZT BESTELLEN:
ct.de/digital

Quelle: Gunnar Jacobson

Öffentlich zugängliche Server übernehmen das Schlüssel- und Zertifikatsmanagement (Abb. 2).

sierte Speichersysteme. Auch hier sollte man sich nicht auf die Transportverschlüsselung und eine serverseitige Chiffrierung verlassen, denn der Cloud-Betreiber hat dann immer eine Möglichkeit zum lesenden Zugriff. Beispiele für ein effizientes End-to-End in der Cloud sind Boxcryptor auf der Basis von Passwörtern sowie certDrive auf der Basis von digitalen Zertifikaten.

Eine weitere populäre Anwendung ist Instant Messaging (IM), also die spontane Übermittlung von Textnachrichten im Push-Verfahren (Chat). Verbreitet sind im privaten Umfeld WhatsApp und im geschäftlichen Bereich Microsoft Lync. Während Lync keine Ende-zu-Ende-Verschlüsselung bietet, gibt es hierzu zahlreiche IM-Anwendungen wie Threema oder TextSecure. Der große Nachteil solcher IM-Dienste ist, dass sie kaum interoperabel sind. Ob das Off-the-Record Messaging Protocol (OTR) dies ändert, bleibt abzuwarten.

Beim E-Mail-Verkehr kann man hingegen Interoperabilität als Selbstverständlichkeit voraussetzen – auch was die Verschlüsselung mit S/MIME (Secure/Multipurpose Internet Mail Extensions) angeht. Andere Verfahren wie Identity Based Encryption (IBE) oder auch XML Encryption konnten sich hier nicht durchsetzen.

Geheimbotschaften waren schon immer gefragt

Die Verschlüsselung von Nachrichten war schon zu Zeiten Julius Cäsars eine wichtige militärische Aufgabe, und das Brechen der deutschen Enigma-Codes durch Alan Turing hat den Zweiten Weltkrieg vermutlich um einige Jahre verkürzt. Ein Hauptproblem solcher symmetrischer Verschlüsselungsverfahren ist der sichere Austausch der Schlüssel. Dieses Problem schien in den 1970er Jahren gelöst, nachdem Diffie und Hellman das Prinzip der asymmetrischen (Public Key) Kryptografie und Rivest, Shamir und Adleman das nach ihren Initialen benannte, vor allem in der E-Mail-Kommunikation praktisch nutzbare RSA-Verfahren vorstellten. Man konnte nun also seinen Public Key veröffentlichen, mit dem jedermann in der Lage war, Nachrichten an einen zu verschlüsseln, während man selbst diese nur mit dem Private Key dechiffrieren konnte. Nebenbei lässt sich mit dem privaten Schlüssel eine digitale Signatur erzeugen. Der Empfänger kann dann anhand des Public Keys die Authentizität der Nachricht feststellen.

Da asymmetrische Kryptoverfahren rechenintensiv sind, verwendet man meist eine Kombination, die hybride Verschlüsselung. Symmetrische Verfahren wie 3DES oder AES werden dabei mit einem Data Encryption Key (DEK) zur Datenverschlüsselung eingesetzt. Der DEK wird mit den Public Keys der Empfänger verschlüsselt und zusammen mit der Nachricht übertragen. Public-Key-Verfahren haben somit zwei Hauptanwendungsgebiete: Schlüsselverteilung und digitales Signieren.

Aufgaben der Public-Key-Infrastruktur

Aus kryptologischer Sicht waren Public-Key-Verfahren ein Durchbruch, dennoch hat sich E2EE bis heute nicht in der Breite durchgesetzt. Was sind die Voraussetzungen für eine stärkere Verbreitung? Zunächst muss die Verschlüsselung rechtlich zulässig sein und darf nicht durch Gesetzeslücken ausgehebelt werden. Darüber hinaus sollte sie für den Benutzer völlig transparent erfolgen. Und schließlich muss der Aufwand für ein Public-Key-System so gering wie möglich gehalten werden.

Um diese Kriterien zu erfüllen, bedarf es einiger technischer Anforderungen: Der Public Key des Empfängers muss überall verfügbar sein und eindeutig seinem Besitzer zugeordnet werden können. Seine Gültigkeit muss sich zweifelsfrei bestimmen lassen. Der Besitzer sollte vollständige Kontrolle über seinen Private Key haben, der auch immer dort verfügbar sein muss, wo man ihn benötigt, und bei Verlust wiederhergestellt werden kann. Zudem sollten die Prozesse zur Schlüsselverwaltung weitgehend automatisierbar sein. Und nicht zuletzt muss das ganze Verfahren interoperabel sein, das heißt: Absender und Empfänger können unterschiedliche Produkte und Dienstanbieter verwenden. Diese Anforderungen an die Schlüsselverwaltung werden durch eine Public-Key-Infrastruktur (PKI) erfüllt.

Kann man einem Public Key vertrauen?

Neben den kryptografischen Eigenschaften ist das wichtigste Merkmal eines Public Keys die eindeutige Zuordnung zu seinem Besitzer, beispielsweise in Form einer E-Mail-Adresse. Wenn es jemandem gelingt, einen Public Key mit der Adresse einer anderen Person zu verteilen, wird er die für diese Person verschlüsselten E-Mails lesen können, der vorgesehene Empfänger aber nicht mehr. Solche Vorfälle sind im Fall von PGP-Verschlüsselung (Pretty Good Privacy) bekannt.

Um das Vertrauen in Public Keys zu stärken, werden verschiedene Verfahren angewandt. Das einfachste beruht auf bilateralem Vertrauen:

Die Kommunikationspartner A und B tauschen gegenseitig ihre Public Keys, beispielsweise auf einer Krypto-Party. Erweitern lässt sich diese Konstellation durch ein Vertrauensgeflecht (Web of Trust): Der Partner B, dessen Public Key Partner A bereits vertraut, bestätigt das Vertrauen in den Public Key einer weiteren Person C durch eine digitale Signatur. Somit kann A auch dem Public Key von C vertrauen. Schließlich ergibt sich eine weiter gefasste Vertrauenshierarchie: Die Glaubwürdigkeit von Public Keys wird durch eine Certification Authority (CA) hergestellt, der alle Teilnehmer vertrauen. Die CA signiert ein digitales Zertifikat gemäß ITU X.509, das neben dem Public Key auch den Namen sowie weitere Attribute enthält (X.509-Zertifikate bieten daneben auch die Option der Sperrung eines Public Keys durch die CA). Alle Teilnehmer haben die Möglichkeit, das Zertifikat anhand des Public Keys der CA zu prüfen. Eine CA kann auch selbst ein Zertifikat durch eine übergeordnete CA erhalten. Die Vertrauenshierarchie endet schließlich an einer sogenannten Root CA.

Bei all diesen Verfahren wird das Vertrauen in Public Keys, vor der eigentlichen Anwendungskommunikation, offline hergestellt. Während des Anwendungsprotokolls führt der Client eine Validierung des Public Keys durch. Bei vielen proprietären E2EE-Anwendungen im Bereich von Instant Messaging oder Cloud Encryption wird das Vertrauen in Public Keys durch den Dienstanbieter online hergestellt. Der Service liefert im Protokollablauf dem Client den benötigten Public Key des Partners zurück (ein Beispiel hierfür wäre Apple iMessage). Hierbei muss man allerdings dem Dienstanbieter vollständig vertrauen. Denn dieser kann sich durch Verteilung vorgetäuschter Keys Zugriff auf alle über seinen Server ausgetauschten Daten verschaffen.

Eine deutliche Anhebung des Sicherheitsniveaus wird erst durch eine strikte Trennung von Anwendungs- und Schlüsseldienst geschaffen: Ein vertrauenswürdiger Schlüsseldienst stellt dem Client die benötigten Public Keys bereit, die er zuvor zentral validiert hat. Er entlastet damit den Client von dieser komplexen Aufgabe. Der Schlüsseldienst hat selbst keinen Zugriff auf die ausgetauschten Nachrichten und ebenso, mangels Schlüssel, auch der Anwendungsdienst nicht.

Das erste Verfahren ist zuverlässig, aber aufwendig und kommt daher zwar im privaten, nicht aber für den betrieblichen Einsatz infrage. Das zweite Verfahren kommt bei PGP zum Einsatz. Die CA-kontrollierte Vertrauenshierarchie ist das heute für Organisationen bevorzugte Modell. Diese können hiermit das Vertrauen in alle internen Public Keys regeln – nicht nur für Personen, sondern auch für Geräte und Dienste. Oft kommt hier eine Windows-PKI zum Einsatz. Das Vertrauen in die PKI anderer Organisationen kann dann entweder durch eine Kreuz-Zertifizierung der CAs oder durch die Teilnahme in einer Bridge CA hergestellt werden, die beispielsweise eine Certificate Trust List bereitstellt. Ein sehr erfolgreiches Beispiel hierfür ist die TeleTrusT European Bridge CA (EBCA).

CA-Dienste stellen auch kommerzielle Anbieter (Trust Service Provider) wie Symantec, QuoVadis oder SwissSign bereit. Mithilfe der Managed-PKI-Dienstleistungen dieser Anbieter werden Unternehmen mit Zertifikaten versorgt. Der Vorteil dabei ist, dass die zugehörigen Root-

Quelle: Gunnar Jacobson

Eine Integration sämtlicher Endgeräte schließt die letzten Lücken in der Verschlüsselungskette (Abb. 3).

Zertifikate in vielen Systemen bereits vorkonfiguriert sind und der Public Key des Anwenders damit global als vertrauenswürdig gilt.

Wie kommt man an die Public Keys?

Verschlüsselung muss spontan und ohne Aufwand für jeden Empfänger möglich sein. Einem Anwender kann nicht zugemutet werden, dass er sich die Public Keys seiner Partner manuell besorgt, in seinem lokalen Adressbuch speichert und als vertrauenswürdig markiert. Digitale Zertifikate kann man in einem extern erreichbaren Zertifikatsserver veröffentlichen, der über eine LDAP-Anwendung (Lightweight Directory Access Protocol) abgefragt wird. Er stellt die internen Zertifikate abgesichert im Internet bereit und dient ferner als Zertifikatssuchmaschine. Gängige Clients wie Microsoft Outlook, die LDAP unterstützen, aber auch mobile Endgeräte wie das iPhone können über das ActiveSync-Protokoll hierüber automatisiert suchen.

Die Validierung der gefundenen Zertifikate kann der Zertifikatsserver zentral übernehmen, er liefert dem Client dann nur gültige Zertifikate zurück. Alternativ lässt sich über ein HTML-Formular auch manuell nach Zertifikaten für eine E-Mail-Adresse suchen. Nach X.509-Zertifikaten und PGP-Keys kann man beispielsweise auf certbox.org oder auf pgp.mit.edu (MIT-Keyserver) recherchieren. Ein für den Datenschutz äußerst wichtiges Merkmal ist dabei die Eigenschaft, nur auf gültige Adressanfragen zu antworten und ein unberechtigtes Abgreifen von E-Mail-Adressen (Address Harvesting Attacks) sowie weiterer organisationsinterner Daten zu verhindern. Leider haben nur wenige öffentliche Key- und Zertifikatsserver diese Eigenschaft. Auch andere Verfahren wie Public Key Pinning oder DNSSEC muss man in dieser Hinsicht sorgfältig überprüfen (Abbildung 2).

Bevor ein Public Key veröffentlicht werden kann, muss zunächst ein Schlüsselpaar generiert werden. In einer Windows PKI übernehmen das die Clients. Die Zertifikatsausstellung kann in mehrstufigen manuellen Genehmigungsprozessen bis hin zum völlig benutzertransparenten Auto-Enrollment erfolgen. Die Option, private Schlüssel durch autorisierte Instanzen zu rekonstruieren, ist dabei für Unternehmen unerlässlich, um Daten bei Schlüsselverlust oder nach dem Ausscheiden eines Mitarbeiters wieder lesbar zu machen.

Sicher Verschlüsseln – auch mit dem Smartphone

Wie schafft man nun aber den Private Key bequem und sicher auf alle eigenen Endgeräte, damit man überall seine E-Mails entschlüsseln kann? Aus Sicht des Benutzers und der IT-Sicherheit wäre eine Smartcard ideal, kombiniert mit einem multifunktionalen Mitarbeiterausweis, den man immer bei sich trägt. Die Unterstützung von Smartcards unter Windows ist gewährleistet, auf Mobilgeräten aber begrenzt und teuer.

Softwareschlüssel werden von Windows und gängigen Mobilgeräten unterstützt und zugriffsgeschützt gespeichert. Die Herausforderung ist hier, den einmal erzeugten Private Key eines Benutzers samt Zertifikat auf all seine Geräte zu verteilen. Das kann beispielsweise durch einen Push-Dienst realisiert werden, der die Keys verschlüsselt auf die Geräte sendet. Am Ende ist dann der Benutzer in der Lage, auf jedem seiner Geräte Nachrichten zu ver- und entschlüsseln.

KONTRÄRE ANFORDERUNGEN BEI MITTEILUNGEN

Business E-Mail	Privater Chat
Nicht-Abstreitbarkeit: Der Empfänger möchte den Urheber gegenüber Dritten nachweisen.	*Abstreitbarkeit:* Im Chat will keiner, dass eine Aussage gegen ihn verwendet werden kann.
Key Recovery: Ein Unternehmen muss E-Mails jederzeit kontrolliert lesbar machen können.	*Forward Secrecy:* Chats sind flüchtig. Ein geknackter Schlüssel soll nicht für alte oder künftige Chats genutzt werden können.
Organisiertes Vertrauen: Schlüsseln muss innerhalb der Organisation vertraut werden.	*Bilaterales Vertrauen:* Schlüssel werden direkt mit dem Partner ausgetauscht.
Interoperabilität: Herstellerunabhängigkeit und Investitionssicherheit stehen im Vordergrund.	*Proprietäre Lösung:* Man einigt sich auf die beste App.

Windows CA oder Managed PKI?

Windows Server bringt eine komplette PKI mit sich, die sich mit wenigen Mausklicks installieren lässt. In puncto Sicherheit wird man aber bei einer Online Enterprise CA an Grenzen stoßen. Angreifer mit Insiderwissen oder mit fortgeschrittenen Fähigkeiten und Tools können eine ernsthafte Bedrohung darstellen. Berichte über solche Angriffe häufen sich. Der Angriff auf die CA von DigiNotar im Jahr 2011, der letztlich zur Liquidation der Firma führte, lief übrigens trotz verwendetem Hardware Security Module (HSM) erfolgreich ab.

Um direkte Angriffe auf die interne CA und deren private Schlüssel zu verhindern, gibt es nur einen effektiven Weg: Die CA muss von dem produktiven Netzwerk und vom Active Directory (AD) isoliert werden. Damit trotzdem weiterhin aus dem Produktiv-AD manuell oder automatisiert Zertifikate beantragt und ausgestellt werden können, sollte ein Certificate Enrollment Proxy in das AD integriert werden, der eine abgesicherte Verbindung zur eigentlichen CA unterhält. Wenn man der Microsoft Software nicht vertraut und Backdoors in der Windows CA befürchtet, kann man so beispielsweise andere CA-Produkte aber auch Open Source CAs wie OpenSSL, OpenXPKI oder Dogtag anbinden.

Über einen solchen Proxy lässt sich auch die CA eines öffentlichen Trustcenters anbinden. Damit stehen einem die Dienste einer Managed PKI zur Verfügung. Das hat den enormen Vorteil, dass die Zertifikatsausstellung nicht umständlich manuell über ein Web-Portal stattfinden muss, sondern dass ein Auto-Enrollment von weltweit anerkannten Zertifikaten für interne Benutzer sowie Windows- und Mobilgeräte erfolgen kann. Benutzer sind somit in der Lage, mit einem öffentlichen, anerkannten Zertifikat auf all ihren Geräten (Any-to-Any) beispielsweise verschlüsselte E-Mails (Ende-zu-Ende) auszutauschen (Abbildung 3).

Fazit

Nach heutigem Stand der Technik sind alle Technologien und Dienste verfügbar, die eine interoperable Any-to-Any-Verschlüsselung ermöglichen. Sie müssen zum Schutz vor Cyberspionage und Hackerangriffen einfach nur intensiver genutzt werden – und das nicht nur in Großkonzernen, sondern insbesondere auch in der IT-Infrastruktur mittelständischer Unternehmen.

Dr. Gunnar Jacobson
Geschäftsführer Secardeo GmbH

Referenzen

[1] Corporate Trust: Studie: Industriespionage 2014, Cybergeddon der deutschen Wirtschaft durch NSA & Co.?
[2] Shirey: RFC 4949, Internet Security Glossary, Version 2, IETF 2007.
[3] Borisow, Goldberg, Brewer: Off-the-record communication, or, why not to use PGP, Proceedings of the 2004 ACM workshop on Privacy in the electronic society, ACM 2004.
[4] Ramsdell, Turner: RFC 5751, Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification, IETF 2010.
[5] Schmidt: Die Schlüssel-Falle – Gefälschte PGP-Keys im Umlauf, c't 6, Heise Verlag 2015.
[6] ITU: Open systems interconnection – The Directory: Public-key and attribute certificate frameworks, ITU 2012.
[7] Jacobson, Neppach: Zertifikatsverzeichnisse für „öffentliche" Public Keys, DuD 7/2009, Gabler 2009.

Kritische Infrastrukturen brauchen schärferen Schutz

Der geplante Schutz ziviler Versorgungsnetze deckt bislang noch nicht alle sicherheitsrelevanten Bereiche ab

Als Industrieland steht Deutschland angesichts der Energiewende und der vierten industriellen Revolution (Stichwort: Industrie 4.0) vor grundstürzenden Paradigmenwechseln. Ohne eine ausreichende und verbindliche Absicherung aller verwendeten Systeme werden wir volkswirtschaftlich erpressbar.

Mit dem Umsetzungsplan KRITIS hat Deutschland europäische Überlegungen zwar schon frühzeitig, aber dennoch nur zum Teil übernommen. Frühzeitig, weil die Bundesrepublik eines der ersten EU-Länder war, die eine nationale Strategie zum Schutz kritischer Infrastrukturen gegen Cyberrisiken aufgebaut hat. Dabei wurden diese volkswirtschaftlich bedeutenden Bereiche in neun Sektoren aufgeteilt: Energie, Gesundheit, Informations- und Kommunikationstechnik, Transport und Verkehr, Medien und Kultur, Wasser, Finanzdienstleistungen, Ernährung sowie Staat und Verwaltung.

Auswirkungen des IT-Sicherheitsgesetzes

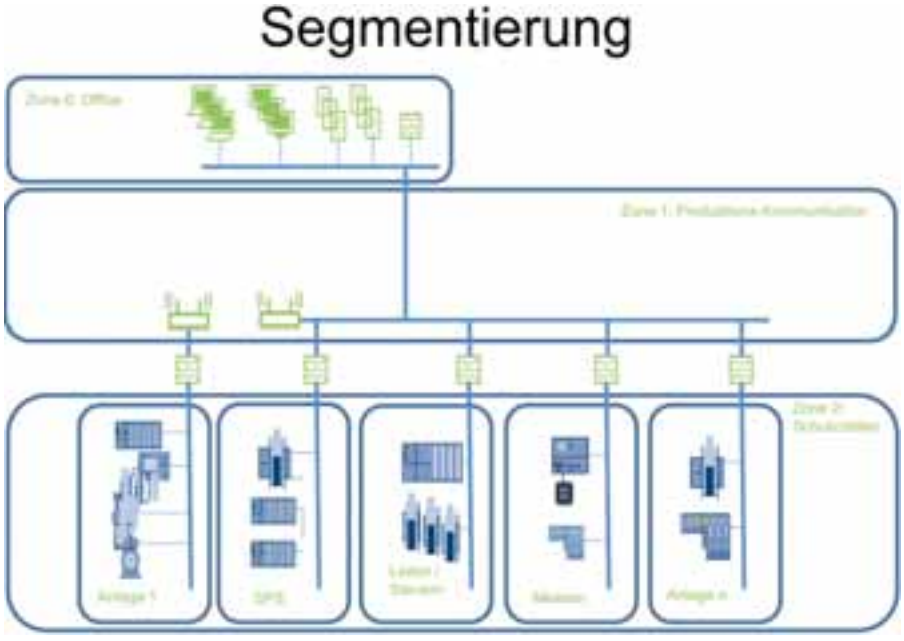
Die organisatorische Umsetzung in Form einer selbstständigen Einheit bleibt zunächst im Wesentlichen auf die Kompetenzen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) beschränkt, das streng genommen nur für Bundesbehörden zuständig ist. Auch wenn das dadurch neu geschaffene Cyberabwehrzentrum formal eigenständig ist, untersteht es dennoch dem BSI-Präsidenten. Zunächst war es nur mit einem Dutzend Mitarbeitern besetzt. Das reicht natürlich für eine übergreifende Zuständigkeit nicht aus, auch wenn eine solche Institution von der engen Zusammenarbeit mit dem BSI, aber auch anderen Behörden und Institutionen profitiert.

Das geplante IT-Sicherheitsgesetz ist ein „Artikelgesetz", das einzelne Artikel in einer Reihe von Bundesgesetzen betrifft. Dazu gehören beispielsweise Gesetze zur Aufgabenbeschreibung des BSI, des Bundeskriminalamts (BKA) oder des Bundesamtes für Bevölkerungsentwicklung und Katastrophenschutz (BBK). Des Weiteren sind Änderungen am Energiewirtschaftsgesetz oder am Telemediengesetz vorgesehen.

Doch vor allem die Position des BSI ändert sich entscheidend. In der Fassung des Referentenentwurfs vom 4.11.2014 wird für das BSI-Gesetz u.a. folgende Ergänzung vorgesehen: „Das Bundesamt ist zuständig für die Informationssicherheit auf nationaler Ebene." Damit ist eine erhebliche Kompetenzerweiterung verbunden, die das BSI zur

Quelle: Willi Kafitz

Das IT-Sicherheitsgesetz ist Teil der Digitalen Agenda der Bundesregierung. Für Energieversorger wird es durch den IT-Sicherheitskatalog der BNetzA flankiert (Abb. 1).



Quelle: Unify GmbH & Co. KG 2015

Durch eine Aufteilung in Schutzzonen lassen sich gefährdete Produktionsbereiche erfassen (Abb. 2).

Fachaufsicht über IT-Sicherheitsbelange von nationaler Bedeutung macht (Abbildung 1).

Die Fachaufsicht des BSI

Zunächst geht es vor allem um sicherheitskritische Belange, die staatliche Institutionen betreffen oder unmittelbar hoheitliche Bedeutung haben. Dazu gehört die sichere Kommunikationsanbindung der deutschen Botschaften im Ausland und der Bundesbehörden im Inland. Andere Beispiele wären etwa Vorgaben für Ausweisdokumente (elektronischer Reisepass/Personalausweis) oder für Aufenthaltstitel (Aufenthaltserlaubnis). Ebenfalls betroffen sind technische Richtlinien, z.B. für Chipkarten und Lesegeräte, die qualifizierte elektronische Signaturen und andere Hochsicherheitstechniken anbelangen. Hier hat das BSI die Fachaufsicht über akkreditierte Prüfinstanzen, die Sicherheitsstandards testieren, welche wiederum Voraussetzung zur Marktzulassung von Komponenten sein können.

Ein besonderer Fall war die Amtshilfe des BSI für das Bundeswirtschaftsministerium (BMWi), um Sicherheitsrahmenbedingungen für ein Smart Meter Gateway (SMGW) zu definieren. SMGWs bilden zukünftig eine dezentrale Komponente im „Internet der Energie“. Sie sind besonders schützenswert, da sie zwar als bedeutender Baustein eines TCP/IP-Netzes im Rahmen der Energiewende fungieren, in der Regel aber in kaum geschützter Umgebung installiert werden, wie etwa heutige Strom- und Gaszähler.

Der Bundesverband IT-Sicherheit e.V. (TeleTrusT), vertreten durch die Arbeitsgruppe „Smart Grids/Industrial Security“, hat diesen Prozess von Anfang an begleitet und im letzten Jahr ein Positionspapier zur Sicherheit im Smart Grid vorgelegt. Wir haben dabei die aktive Mitarbeit des BSI beim Thema Sicherheit für kritische Infrastrukturen begrüßt. Insgesamt ist jedoch noch viel Arbeit zu leisten (Abbildung 2).

Bedrohung durch Cyberattacken

Die Energienetze von heute – und erst recht die angestrebten intelligenten Energienetze von morgen (Smart Grids) – müssen mit höchster Priorität gegen Cyberangriffe abgesichert werden. Das zeigen aktuelle Beispiele, bei denen nur mit viel Glück womöglich verheerende Attacken abgewehrt werden konnten. So fand sich zum Jahreswechsel 2013/2014 eine ausgeklügelte Malware bei über 1000 Energieversorgern in 84 Ländern, eingeschleust von der Hackergruppe „Dragonfly“. Offenbar in staatlichem Auftrag wurden digitale Zeitbomben in die Netze implementiert, die die Angreifer aus Osteuropa quasi per Mausklick hätten zünden können. Und erst kürzlich warnte das amerikanische Computer Emergency Response Team (CERT) vor einer neuen gefährlichen Malware namens „Black Energy“, die ebenfalls die Energie- und Wasserwirtschaft bedrohte. Ähnliche Beispiele finden sich in allen neun Sektoren kritischer Infrastrukturen.

Mit erfolgreichen Angriffen auf den Hamburger Senat und dem Datendiebstahl von 270.000 Fahndungsdatensätzen bei der Bundespolizei war auch der Sektor „Staat und Verwaltung“ betroffen. Umso erstaunlicher ist es, dass dieser Bereich im Entwurf des IT-Sicherheitsgesetzes zur ersten Lesung im Bundestag am 20.03.2015 ausgeklammert wur-

Quelle: Unify GmbH & Co. KG 2015

Die Einsatzzyklen vernetzter Anlagen können stark voneinander abweichen (Abb. 3).

Quelle: Unify GmbH & Co. KG 2015

Schwachstellen in Unternehmensnetzen schaffen Lücken für vielfältige Bedrohungen (Abb. 4).

de und somit nicht dem Meldewesen und der Pflicht zu einem überprüfbaren Mindestsicherheitsniveau unterliegt.

Das IT-Sicherheitsgesetz ist als Bundesgesetz ausgelegt und könnte zumindest die Verwaltungen des Bundes adressieren. Einige Verbände haben bereits gefordert, dass hier der Gesetzentwurf nachgebessert wird. Bis alle Anforderungen tatsächlich umgesetzt sind, kann immer noch eine Priorisierung erfolgen. Das Gesetz soll die Betreiber kritischer Infrastruktur befähigen, sich besser gegen Cyberangriffe zu wappnen und solidarisch mögliche Gefahren im allgemeinen Interesse zu melden. Doch das darf keine Einbahnstraße bleiben. Gleichzeitig muss auch jede betroffene staatliche Institution die Sicherheitslage auf Relevanz für das eigene Haus einschätzen können. Das IT-Sicherheitsgesetz soll schließlich die Innere Sicherheit der Bundesrepublik Deutschland stärken, weil die Abhängigkeit von Informations- und Kommunikationstechnologie (IKT) so groß geworden ist, dass ein Ausfall in diesem Sektor erhebliche volkswirtschaftliche Schäden nach sich ziehen kann.

Reichen die geplanten Maßnahmen aus?

Deutschland steht vor gleich mehreren Paradigmenwechseln. Neben der Energiewende sind die zukünftigen intelligenten Netze ein besonders schützenswerter Bereich, weil die Abhängigkeit von IKT noch erheblich größer werden wird, als es heute schon der Fall ist. Sicher gehören die KRITIS-Sektoren Ernährung, Gesundheit, Wasser, Finanzdienstleistungen, die Mobilität, die Kommunikationsfähigkeit und die Möglichkeit, sich über Medien zu informieren, zu den elementaren nationalen Infrastrukturen. Doch auch Staat und Verwaltung müssen sich am gleichen Maßstab messen lassen. Und angesichts weiterer Megatrends muss man sich fragen, ob das ausreicht.

Infrastrukturen werden dann als kritisch eingestuft, wenn ihre Betreiber nicht einem normalen betriebswirtschaftlichen Risikomanagement unterliegen dürfen. Natürlich ist es eine Frage des freien unternehmerischen Risikos, ob Cyberrisiken eliminiert, reduziert, ignoriert oder versichert werden. Im volkswirtschaftlichen Interesse darf der Staat jedoch mehr fordern. Eine Regulierung des Sicherheitsniveaus muss erfolgen, wenn eine organisationsübergreifende digitale Vernetzung starke, kaum beeinflussbare gegenseitige Abhängigkeiten schafft (Abbildung 3).

Auf genau diese Entwicklung bezieht sich der seit wenigen Jahren geprägte Begriff „Industrie 4.0“. Er beschreibt den Weg zu einer grundlegend veränderten, digitalisierten Produktionsweise, die einer vierten industriellen Revolution gleichkommt. Sie ist nicht vergleichbar mit den bereits heute schon bestehenden Kommunikationsbeziehungen, die Firmen (meist bilateral) zu Behörden, Zulieferern, Partnern oder Kunden aufgebaut haben. Diese Beziehungen können vertraglich, organisatorisch und technisch durch jeden der Partner in voller Souveränität abgesichert werden. Ganz anders verhält es sich aber mit vernetzten und synchronen Strukturen auf der Grundlage von Cyber Physical Systems. Sie bilden die Basis für noch komplexere Geschäfts- und Betriebsprozesse.

In einer kürzlich erschienen IDC-Studie heißt es: „In der Vision einer vollständigen Durchdringung der Industrie 4.0 besteht die Produktionsumgebung aus intelligenten, vernetzten Objekten, die den Fertigungsprozess weitgehend autonom durchlaufen und deren Daten die Grundlage für Analysen, ein durchgängiges Engineering und intelligente Wertschöpfungsketten bilden.“ Basis und Umfeld dieser Entwicklung wird ein stabiles, schnelles und sicheres Internet sein. Wie die oben genannten Sektoren mit kritischen Infrastrukturen, zu denen fraglos die Informations- und Kommunikationsinfrastrukturen zählen, wird man auch die Branchen und Sektoren um Industrie 4.0 mittelfristig erweitern müssen. Ohne ausreichende Sicherheit wird Deutschland sonst gerade in dieser Kernkompetenz volkswirtschaftlich erpressbar (Abbildung 4).

Fazit

Aus Sicht des Bundesverbandes IT-Sicherheit e.V. (TeleTrusT) begrüßen wir gesetzliche Regelungen bei der IT-Sicherheit, die sich für den Energiesektor ohnehin bereits abzeichnen. Gleiches muss auch für andere Sektoren gelten. Besonders der Bereich „Staat und Verwaltung“ sollte bei der Gesetzgebung keinesfalls ausgeklammert werden. Auch die rasante Entwicklung bei der IKT darf nicht unterschätzt werden. Schneller als man denkt und der Bundestag Gesetze erlassen kann, wird die Business-to-Business-Kommunikation (B2B) im Rahmen der Industrie 4.0 von so zentraler volkswirtschaftlicher Bedeutung sein, dass regulatorische Sicherheitsvorgaben erforderlich werden. Gegebenenfalls muss man auch sie als kritische Infrastruktur einstufen.

Nach dem heute vorliegenden Gesetz hat das dann zwei Konsequenzen für alle Beteiligten: Einhaltung eines Mindestsicherheitsniveaus und Mitwirkung am nationalen Meldewesen für Cyberangriffe. Angesichts der vierten industriellen Revolution in einem der wichtigsten Industrieländer dieser Welt sollte das nicht zu viel verlangt sein.

Dr. Willi Kafitz
TeleTrusT – Bundesverband IT-Sicherheit e.V.,
Arbeitsgruppe „Smart Grids/Industrial Security“
und Arbeitsgruppe EBCA-AG „Technik“

Nach innen und außen zuverlässig geschützt

Kombinierte Verschlüsselungsverfahren erfüllen sowohl Sicherheitsbedürfnisse als auch Compliance-Vorgaben

Dass E-Mail-Kommunikation nicht sicher ist, hat spätestens seit Snowdens NSA-Enthüllungen das öffentliche Bewusstsein erreicht. Daten werden im großen Stil kopiert und manipuliert, und niemand bemerkt es. Tatsächlichen Schutz gegen Cyberattacken kann nur eine umfassende PKI-basierte Verschlüsselung bieten.

E-Mails sind als Kommunikationsform längst nicht nur in der Mitte der Gesellschaft, sondern auch flächendeckend in der Wirtschaft angekommen. Ihre breite Verwendung in Unternehmen erklärt sich unter anderem aus ihrer Effizienz. Sie erlauben eine kostengünstige und standortunabhängige Kommunikation in Echtzeit, dokumentieren lückenlos den Kommunikationsverlauf und ermöglichen den einfachen Transport von Dateien ohne Medienbruch. Diese Vorteile möchten Unternehmen nicht missen, auch wenn es oft an der Sicherheit mangelt.

Echte Ende-zu-Ende-Verschlüsselung

Daher trifft der verantwortungsvolle Unternehmer Sicherheitsvorkehrungen, um nicht der Industrie- und Wirtschaftsspionage ausgeliefert zu sein und Firmeninterna zu schützen. Zusätzlich wird vom Gesetzgeber, etwa nach dem Bundesdatenschutzgesetz (BDSG), ein streng geregelter Umgang mit personenbezogenen Daten vorgeschrieben. Auch das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) wartet mit Compliance-Vorgaben auf, die eine Verschlüsselung nach dem Stand der Technik vorschreiben.

Eine Sicherheitsmaßnahme, die oft fälschlicherweise als vollwertiger Ersatz einer Ende-zu-Ende-Verschlüsselung (End-to-End Encryption oder E2EE) gewertet wird, ist die Verschlüsselung der Übertragungskanäle mittels Transport Layer Security (TLS). Damit ist der Einhaltung der Compliance-Regeln im ersten Schritt Genüge getan. Das Problem dabei: Auf den verschiedenen Stationen, die eine E-Mail durchläuft, wird nur der Weg von einem Server zum nächsten verschlüsselt. Den Server selbst passieren die E-Mails im Klartext. Auch im Postausgang und -eingang, den Anfangs- und Endpunkten der Verschlüsselungsstrecke, werden E-Mails unverschlüsselt abgelegt. Nur echtes End-to-End kann hier tatsächlich Sicherheit bieten.

Doch auch die Ende-zu-Ende-Verschlüsselung sollte abhängig vom Anwendungsfall differenziert betrachtet werden. Sie bedeutet die lückenlose Verschlüsselung vom Sendegerät bis zum Empfangsgerät. Die Nachrichten sind also nirgendwo im Klartext abgelegt, weder im Postausgang des Senders noch im Posteingang des Empfängers. Nur die Endnutzer verfügen letztlich über die notwendigen Schlüssel zum Ver- und Entschlüsseln. So lautet jedenfalls die Theorie.

Richtigerweise müsste End-to-End oft mit „Ende-zu-Weiß-nicht-genau“ übersetzt werden, da der Sender keine hundertprozentige Gewissheit darüber hat, dass sich der geheime Schlüssel wirklich nur im Besitz des adressierten Empfängers befindet. Verwendet dieser zum Beispiel ein Verschlüsselungs-Gateway, sieht man das den verwendeten Schlüsseln in der Regel nicht an. Vertrauen in die Unversehrtheit einer echten Ende-zu-Ende-Verschlüsselung kann es entsprechend nur geben, wenn sich beide Kommunikationspartner persönlich die verwendeten Zertifikate gegenseitig verifizieren und zusichern, dass es keine Kopie an anderer Stelle gibt.

Doppelt hält besser

Für den Großteil des internen und externen E-Mail-Verkehrs hat ein Unternehmen im Normalfall kein Interesse an einer durchgängigen Ende-zu-Ende-Verschlüsselung, bei der die geheimen persönlichen Schlüssel nur die jeweiligen Mitarbeiter besitzen. Diese Situation ist in etwa vergleichbar mit den Büroräumen am Firmensitz: Das Unternehmen gibt nicht jedem Mitarbeiter einen exklusiven Schlüssel für sein Büro. Es gibt so etwas wie ein Hausrecht inklusive der Nutzung von Zweit- bzw. Generalschlüsseln.

Genauso soll und muss ein Unternehmen schon aus Compliance-Gründen die Hoheit über die eigenen E-Mail-Daten besitzen. Ohne einen zentralen Zugriff auf den E-Mail-Verkehr ist auch der essenzielle Einsatz von Contentfiltern und Data-Loss-Prevention-Lösungen nicht möglich. Um nicht gänzlich die Kontrolle zu verlieren, müssen sonst flächendeckend Rollouts auf allen Clients organisiert und gepflegt werden.

Auch eine Archivierung ist ohne Nachschlüssel nicht sinnvoll, will man nicht die Archivzuführung ebenfalls dezentral auf den Clients realisieren. Entsprechend werden heute in der Regel in Unternehmen mithilfe von Public-Key-Infrastruktur-Anwendungen Kopien der geheimen Schlüssel der Mitarbeiter oder Generalschlüssel zentral und sicher verwaltet. Dazu gibt es verschiedene technische Ansätze, die im Allgemeinen als Key-Escrow-Verfahren bezeichnet werden.

Die genannten Problemfelder der Ende-zu-Ende-Verschlüsselung lassen sich durch eine einfache Veränderung des Blickwinkels auflösen. Am einen Ende der E-Mail-Verschlüsselung im geschäftlichen Bereich steht das Unternehmen an sich – also die juristische Person. Da die Mitarbeiter im Auftrag der Firma kommunizieren, ist der Sender beziehungsweise Empfänger grundsätzlich das Unternehmen. Deshalb kann die Grenze vom Internet zum Unternehmen als ein Endpunkt der sicheren externen Kommunikation angesehen werden. Zusätzlich sollten Unternehmen aber auch ihren internen Informationsaustausch mit

den eigenen Mitarbeitern wiederum End-to-End verschlüsseln. Dies könnte man dann gewissermaßen als Ende-zu-Ende-zu-Ende-Verschlüsselung bezeichnen.

Basis der Verschlüsselung ist die PKI

Eine wirksame E-Mail-Verschlüsselung basiert auf Public-Key-Infrastrukturen (PKIs). Dafür haben sich mit S/MIME (Secure/Multipurpose Internet Mail Extensions) und OpenPGP zwei Standards etabliert. Beide nutzen im Grunde die gleichen kryptografischen Verfahren. Sie unterscheiden sich jedoch in der Zertifizierung der öffentlichen Schlüssel (Zertifikate) und damit in den Vertrauensmodellen.

Der Enrollment-Prozess für X.509-Zertifikate, der für S/MIME eingesetzt wird, sieht vor, dass Schlüsselpaare beim Nutzer (im Unternehmen) generiert werden. Der private Schlüssel verbleibt dort, der öffentliche Schlüssel wird damit signiert und einer Certification Authority (CA) zur Zertifizierung übergeben. Die CA fügt dem öffentlichen Schlüssel ihre eigene Signatur hinzu und sendet den signierten öffentlichen Schlüssel zurück. Ab diesem Moment wird ein öffentlicher Schlüssel zum Zertifikat. Bei PGP signieren und zertifizieren sich die User ihre Schlüssel auf Basis persönlicher Kontakte gegenseitig und bilden damit ein Vertrauensnetzwerk (Web of Trust).

PKIs bauen darauf, dass Zertifikate breit gestreut werden, Dritte jedoch zu keinem Zeitpunkt Zugriff auf persönliche Schlüssel erhalten. Der Einsatz des Key-Escrow-Verfahrens innerhalb der Unternehmenskommunikation bleibt davon unberührt und sorgt für die Erfüllung von Compliance-Anforderungen, Zugriffsmöglichkeiten für zentrale Contentfilter, Data Loss Prevention (DLP) und Archivlösungen sowie die Datenhoheit des Unternehmens.

Schutz nach innen

Die beiden Verschlüsselungsmethoden S/MIME und PGP sind nicht miteinander kompatibel. Die Entscheidung im Unternehmen für einen Standard führt somit dazu, dass Verschlüsselung nur möglich ist, wenn der Kommunikationspartner genau denselben Standard nutzt. Im Unternehmensbereich hat sich S/MIME, in Kombination mit X.509-Zertifikaten, die durch Trustcenter oder im eigenen Unternehmen ausgestellt werden, vor der PGP-Verschlüsselung etabliert.

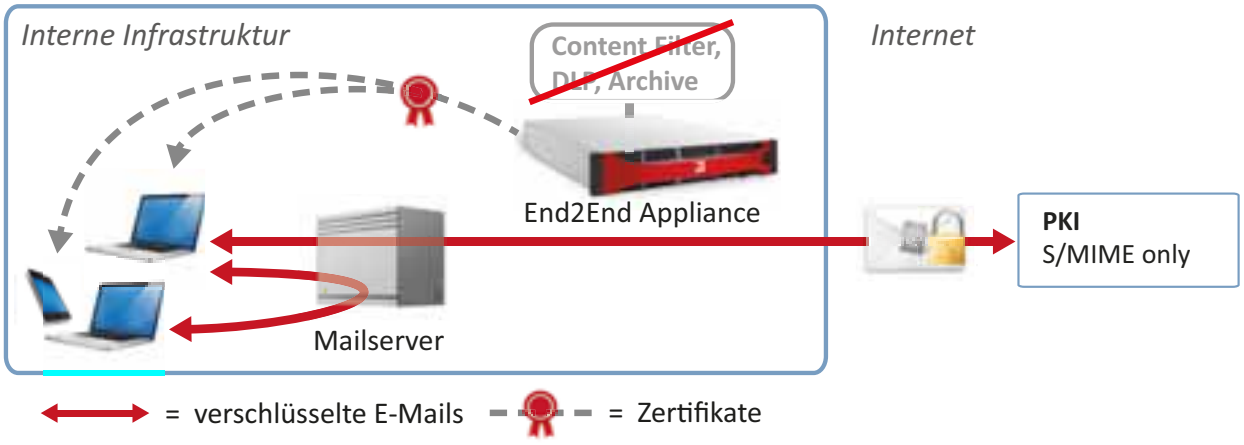
Wird PGP im Unternehmensumfeld genutzt, ist der Vertrauensaufbau in der Regel trotzdem hierarchisch. Anstelle einer breit angelegten Kreuz-Zertifizierung zwischen den einzelnen Mitarbeitern, gibt es einen zentralen Signer Key des Unternehmens, der analog einer CA im S/MIME-Umfeld alle PGP-Schlüssel der Mitarbeiter signiert. Damit wird allen anderen internen und externen Nutzern signalisiert, dass dieser Schlüssel nicht von irgendwem außerhalb des Unternehmens gefälscht wurde. Die Nutzung von PGP verlangt darüber hinaus eine Installation zusätzlicher Software auf den Clients. Denn der PGP-Standard wird anders als S/MIME von den heute im Unternehmensumfeld genutzten nativen E-Mail-Clients nicht generell unterstützt.

In der privaten E-Mail-Kommunikation ist – wenn überhaupt – die kostenfreie Verschlüsselung mit OpenPGP verbreitet. Auch kündigen große, im Privatkundenbereich relevante E-Mail-Provider, aktuell die Unterstützung von OpenPGP in ihren Web-Mail-Clients an. So ist davon auszugehen, dass insbesondere für Business-to-Customer-Szenarien (B2C) die Unterstützung von OpenPGP für Unternehmen in Zukunft wichtiger wird.

Sicherheit nach außen

Zum Verschlüsseln einer E-Mail wird bei PKI-basierten Methoden das Zertifikat (der öffentliche Schlüssel) des Empfängers benötigt. Die Nachricht kann nur vom Gegenstück des Zertifikats – nämlich dem privaten Schlüssel des Empfängers – entschlüsselt werden. Diese Zertifikate müssen vor der Verschlüsselung allerdings nicht nur gefunden, sondern auch validiert werden. In einer One-to-One-Situation lässt sich das als manueller Prozess durchführen. Die Kommunikationspartner tauschen die Fingerprints (Prüfsummen der Schlüssel) auf einem sicheren Kanal aus – oft bei persönlicher Begegnung oder durch den Upload auf eine Trustcenter-unabhängige Meta-Zertifikatssuchmaschine wie den Z1 Global TrustPoint – und bestätigen sie gegenseitig. Im geschäftlichen Einsatz, in dem gegebenenfalls eine große Anzahl Mitarbeiter und noch mehr externe Kommunikationspartner Zertifikate austauschen und bestätigen, verlängern und widerrufen, wäre das jedoch enorm aufwendig und langsam.

Wegen des komplexen Schlüssel- und Zertifikatsmanagements hat sich die seit Jahrzehnten verfügbare PKI-basierte Verschlüsselung direkt am Client bisher nicht in der Breite durchsetzen können. Während Privatanwender wahrscheinlich die Mühe scheuen oder wegen fehlendem Sicherheitsbewusstsein auf diese Technologie ganz verzichten, setzen Unternehmen und Organisationen eher auf zentrale Lösungsansätze, sogenannte Secure E-Mail Gateways, um die aufwendige PKI-basierte Verschlüsselung nicht an den vielen internen Clients implementieren zu müssen.



Quelle: Burkhard Wiegel

Bei Personal End-to-End haben Contentfilter ebenso wenig Zugriff auf die E-Mail wie der Gateway-Administrator (Abb. 1).

Gateways automatisieren das interne und externe Schlüssel- und Zertifikatsmanagement und bedienen sich zur Zertifikatssuche und -validierung weitestgehend spezieller Zertifikatsserverkomponenten. Dabei wird Server-basiert – und somit zentral und transparent für die Nutzer – der sicherheitssensible E-Mail-Verkehr gemäß den eingestellten Regelwerken (Policies) geschützt. Compliance Enforcement, eine hohe Nutzer-Akzeptanz sowie der Verzicht auf Client-Installationen sind die Vorteile, die einen Gateway-Einsatz attraktiv machen. Auf diese Weise können Keys sowohl mit X.509-Zertifikaten als auch mit OpenPGP verschlüsselt werden. Falls für externe Kommunikationspartner keine Zertifikate verfügbar sind, verwendet das Gateway alternative Verschlüsselungsmethoden.

Alternativen für Empfänger ohne PKI-Zertifikate

Für zertifikatslose Empfänger gibt es üblicherweise passwortbasierte Verschlüsselungsverfahren. Dabei wird zunächst die Nachricht in einem Puffer zwischengelagert (Spooling) und der Empfänger über die beabsichtigte Zustellung einer vertraulichen E-Mail informiert. Er muss sich dann authentifizieren und erhält die Nachricht beispielsweise als passwortverschlüsselten PDF-, HTML- oder ZIP-Container im E-Mail-Anhang zugestellt. Eine ebenfalls verbreitete Variante der passwortbasierten Verschlüsselung ist die Bereitstellung eines on-the-fly erstellten HTTPS-gesicherten Webmailers. De-Mail-Anbindungen, TLS-Unterstützung und VPN (Virtual Private Network) sind ebenso auf einigen Gateways verfügbar. So können Unternehmen ohne Verzögerung mit jedermann verschlüsselt kommunizieren.

Eine kontrovers diskutierte Option ist die Ad-hoc-Ausstellung von X.509-Zertifikaten für externe Kommunikationspartner. Auch diese Möglichkeit wird manchmal verfolgt, wenn man mit zertifikatslosen Empfängern verschlüsselt kommunizieren will. Der Sender agiert in diesem Fall selbst als CA und stellt on-the-fly Zertifikate und private Schlüssel für externe Nutzer aus. Auf diese Weise erhält der Empfänger in kurzem zeitlichen Abstand die verschlüsselte Nachricht, den privaten Schlüssel und das Zertifikat.

Damit ergeben sich allerdings einige Probleme, da grundsätzliche PKI-Funktionsweisen umgangen werden. Es stellen sich nicht nur heikle Sicherheitsfragen, weil ein Dritter – hier der Ersteller – Kenntnis der privaten Schlüssel der externen Nutzer hat. Es käme auch zu einer inflationären Zertifikatsvermehrung, würde sich dieser Ansatz in der Breite durchsetzen. Denn üblicherweise besitzt ein PKI-Teilnehmer nur ein Zertifikat beziehungsweise eine sehr geringe Anzahl von Zertifikaten, die er allen seinen Kommunikationspartnern zentral verfügbar macht – in etwa vergleichbar mit seiner Telefonnummer. Im Gegensatz dazu bekäme beim eben beschriebenen Ansatz jeder einzelne Mitarbeiter gegebenenfalls von Hunderten seiner Kommunikationspartner wieder jeweils ein separates Zertifikat ausgestellt. Man stelle sich dann nur einmal die vertrackte Situation vor, wenn dieser Nutzer den Arbeitgeber wechselt und damit auch eine andere E-Mail-Adresse erhält.

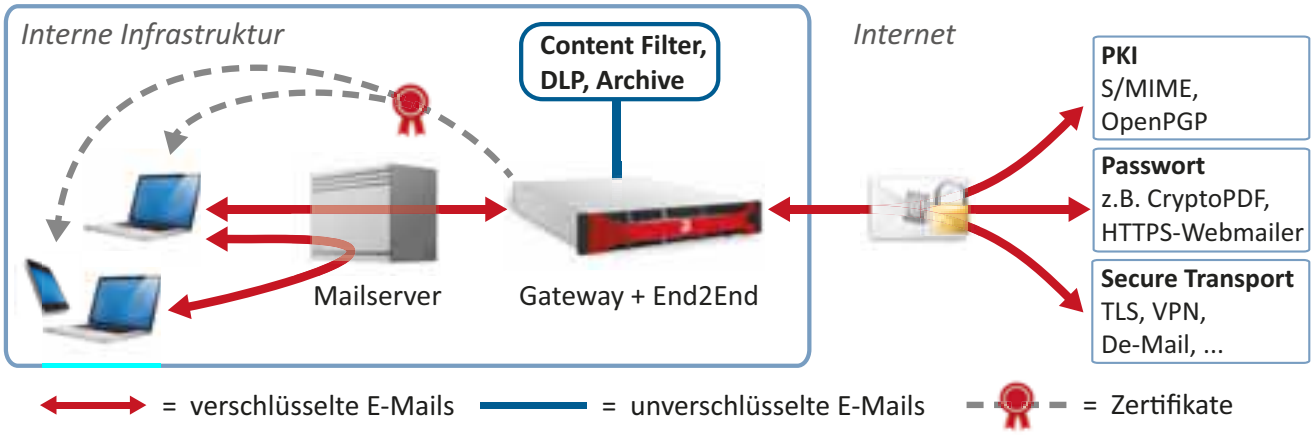
Grenzen der Gateway-Sicherheit

Ein Secure E-Mail Gateway bildet zwar eine zentrale Schnittstelle zum Internet, die von und nach außen ent- bzw. verschlüsselt. Innerhalb des Firmennetzwerkes werden die Nachrichten jedoch unverschlüsselt transportiert. Mit dem Gateway-Ansatz allein nutzen Unternehmen demnach keine klassische Ende-zu-Ende-Verschlüsselung. Für den Schutz gegen Geheimdienstprogramme und Wirtschaftsspionage im Internet ist dies dennoch eine sichere und bewährte Methode. Sie wird seit Jahren erfolgreich von Unternehmen, Behörden und Institutionen eingesetzt. Gleichwohl gibt es Anwendungen, bei denen echtes End-to-End notwendig ist.

Das betrifft beispielsweise die Kommunikation über mobile Endgeräte. Per Notebook, Tablet oder Smartphone ausgetauschte E-Mails werden über WLAN oder Mobilfunknetze im Klartext übertragen. Jede Verschlüsselung über die Transportstrecke Internet ist wirkungslos, wenn ein Angreifer mit etwas IT-Know-how und geringem technischen Equipment über WLAN oder Mobilfunknetze Nachrichten im Klartext abfangen kann. Eine fehlende interne Verschlüsselung erlaubt es außerdem jedem Administrator des Unternehmens mit Zugang zum E-Mail-Server, Inhalte unverschlüsselt auszulesen.

Deshalb gilt es, eine vertrauliche Kommunikation im Unternehmen – das heißt vom Gateway zum einzelnen Mitarbeiter und für den E-Mail-Austausch der Mitarbeiter untereinander – herzustellen. VPNs schützen beispielsweise generell vor Gefahren von außen, bieten aber ähnlich wie TLS nur Verschlüsselung auf Transportebene. Investitionen in Mobile-Device-Management-Systeme (MDM) können dafür sehr lohnend sein. Hierbei ist jedoch eher die Umgebung als Container geschützt und nicht zwingend die einzelne Nachricht. Im MDM-Bereich dominieren zudem Hersteller der „Five-Eyes-Staaten" den Markt. Wer geheimdienstsicher verschlüsseln möchte, strenge eigene Ansprüche oder branchenspezifische Vorgaben zu erfüllen hat, sollte immer das

Quelle: Burkhard Wiegel



Organizational End-to-End gewährleistet eine sichere Kommunikation von und nach außen und sorgt für die notwendige Flexibilität (Abb. 2).

Ziel haben, die Nachrichten und Anhänge selbst zu verschlüsseln und nicht nur ihre Transportwege und Aufbewahrungsorte.

Leider ist nicht davon auszugehen, dass irgendeines der vielen neuen Start-ups in der Verschlüsselungsbranche die Situation in nächster Zeit revolutionieren wird. Deren Ansätze zielen zwar überwiegend auf mobile Endgeräte ab, wenden sich aber vor allem an Einzelanwender und erst in einem zweiten Schritt an Unternehmen. Oft werden dabei die unterschiedlichen Bedürfnisse nicht ausreichend berücksichtigt. Diese Angebote sehen zumeist vor, dass sich Sender und Empfänger bereits kennen und sich gemeinsam auf die Notwendigkeit einer sicheren Kommunikation verständigt haben. In der Regel müssen beide dann auch die gleiche Software installieren und bleiben auf das Endgerät angewiesen, auf dem die Software installiert ist. Eine spontane, effiziente und sichere Kommunikation lässt sich so nicht umsetzen. Zum Teil ist eine sichere Kommunikation auch nur auf bestimmten Betriebssystemen möglich. Derartige Einschränkungen machen den Einsatz für Unternehmen wenig attraktiv.

Personal und Organizational End-to-End

Es bleibt festzuhalten, dass sowohl intern als auch extern verschlüsselt werden sollte. Wenn diese Verschlüsselung in zwei verschiedenen Modi zur Verfügung steht, ist sie in der Tat auch auf breiter Basis unternehmenstauglich.

Im ersten Modus wird die E-Mail komplett durchgängig vom Sender bis zum Empfänger verschlüsselt. Das kann im Einzelfall auf persönlicher Ebene durchaus gerechtfertigt sein und wird deshalb als Personal End-to-End bezeichnet. Dies entspricht der klassischen Form der Ende-zu-Ende-Verschlüsselung. Personal End-to-End dient vor allem der Kommunikation zwischen einzelnen Usern im Hochsicherheitsbereich. Contentfilter und andere Applikationen haben hier keinen Zugriff auf die E-Mail-Inhalte. Ebenso wenig kann der Gateway-Administrator die Nachrichten auslesen oder manipulieren (Abbildung 1).

Für den Einsatz auf breiter Front hingegen eignet sich ein anderer Modus der E-Mail-Übertragung. Hier wird die E-Mail zwischen den Teilstrecken am Gateway umverschlüsselt und der Zugriff für Contentfilter, Virenschutzprogramme u. Ä. gewährt. Das ist ganz im Sinne der einsetzenden Organisation und wird deshalb als Organizational End-to-End betitelt. Im firmeneigenen Netzwerk setzt Organizational End-to-End auf S/MIME. Eine gekapselte, rein interne Public-Key-Infrastruktur dient dem sicheren Nachrichtentransport auf unternehmensinternen Strecken, einschließlich der Verschlüsselung von Nachrichten der Mitarbeiter untereinander. Am Gateway wird die Verschlüsselung unterbrochen und berechtigten Systemen innerhalb der Organisation der Zugriff gewährt. Da die Umverschlüsselung direkt innerhalb des Firmennetzwerkes stattfindet, bleibt ein hohes Sicherheitsniveau gewährleistet. Auf dem E-Mail-Server werden die Nachrichten in verschlüsseltem Zustand abgelegt und sind auf diese Art auch für Administratoren nicht auslesbar.

Von S/MIME, PGP bis zum passwortverschlüsselten PDF oder zum SecureChannel (u. a. TLS oder De-Mail) ist dann eine Abstimmung auf die Infrastruktur des Empfängers möglich. Mit diesem Konzept wird eine sichere Kommunikation von und nach außerhalb gewährleistet und gleichzeitig für die notwendige Flexibilität gesorgt (Abbildung 2).

Bordmittel reichen aus, optionale Plug-ins bieten noch mehr

Nachdem die technischen Herausforderungen betrachtet wurden, darf nicht vernachlässigt werden, auch für eine fehlerfreie Anwendung zu sorgen. Ende-zu-Ende-Verschlüsselung bindet den User mit ein. Abhängig von der Wahl der Clients und eventueller Plug-ins kann der Nutzer Verschlüsselungsaktionen einsehen oder muss sie sogar eigenverantwortlich auslösen.

Da Standard-E-Mail-Clients eigentlich generell S/MIME unterstützen, ist eine Umsetzung mit Bordmitteln, das heißt die Nutzung der nativen Clients, im End-to-End-Szenario problemlos möglich. Ein unternehmensweiter Rollout von Client-Installationen ist daher in der Regel nicht zwingend notwendig. LDAP- (Lightweight Directory Access Protocol) und Active-Sync-Proxies sorgen für den Informationsfluss, der zur Zertifikatsbeschaffung und -validierung benötigt wird. Beim ausschließlichen Einsatz von Bordmitteln trägt allerdings der Endnutzer eine große Verantwortung. Er muss die Verschlüsselung explizit ansteuern und daher entsprechend sensibilisiert und geschult werden. Ein Compliance Enforcement (die Durchsetzung der Unternehmensrichtlinien und -vorgaben) ist beim Einsatz nativer E-Mail-Clients aber nicht möglich.

Sehr viel komfortabler und mit weiteren Mehrwerten angereichert wird die Nutzung von E-Mail-Clients mittels entsprechender Plug-ins. Diese sind gewöhnlich für alle gängigen Client-Programme verfügbar. Sie übersetzen dem User nicht nur die eigentlichen Verschlüsselungsaktionen in einen einfachen Button-Klick, sondern sorgen auch für eine hohe Transparenz beim Zertifikatsmanagement. Verschiedene Verschlüsselungsfunktionen können durch die Abfrage zentraler Policies gesteuert werden. Dadurch wird dann auch ein Compliance Enforcement gewährleistet. Dem User stehen darüber hinaus optional weitere sicherheitserhöhende Aktionen zur Verfügung.

Mithilfe von Plug-ins lassen sich sowohl der gesamte E-Mail-Verkehr wie auch die Einstellungen jedes einzelnen Nutzers sehr einfach über mehrere Endgeräte synchronisieren. Zusätzlich wird Key Escrow – in diesem Fall der zusätzliche, mit einem Escrow Key verschlüsselte Versand – an eine unternehmenszentrale Stelle unterstützt. Das bietet besonders bei Verschlüsselung im Personal-End-to-End-Modus dem Unternehmer die Option, im Notfall an die firmeneigenen Daten zu gelangen. Das Konzept einer kombinierten Verschlüsselung im Organizational und Personal End-to-End-Modus bedient also alle unternehmerischen Anforderungen bei einem Höchstmaß an Sicherheit, Effizienz und Usability.

Fazit

Public-Key-Infrastrukturen bilden ein solides Fundament für den Schutz der E-Mail-Kommunikation im unternehmerischen Bereich. Einzelne Komponenten und unterschiedliche Methoden lassen sich dabei flexibel und anwendungsorientiert kombinieren. Für alle Organisationen, Firmen, Behörden und Institutionen, die nicht ausschließlich kabelgebunden kommunizieren und keine Geheimnisse vor ihren internen Administratoren haben, stellt eine Verschlüsselung per Organizational End-to-End, punktuell ergänzt mit Personal End-to-End, ein universell einsetzbares Lösungskonzept für den sicheren Austausch von schützenswerten Informationen dar.

Unabhängig von der jeweiligen Infrastruktur auf der Empfängerseite und der dort eingesetzten Verschlüsselungstechnik können auf diese Weise Nachrichten in jedem Fall ad hoc verschlüsselt zugestellt werden. Im E-Mail-Verkehr innerhalb des Unternehmens funktioniert das am besten über eine Verschlüsselung per S/MIME. Der Informationsfluss nach außen hin lässt sich zum überwiegenden Teil über ein Secure E-Mail Gateway abwickeln – und das spricht dann im Idealfall alle Sprachen der sicheren E-Mail-Kommunikation.

Dr. Burkhard Wiegel
Geschäftsführer Zertificon Solutions GmbH

Verschlüsselung allein ist nicht alles

Beim Einsatz von Verschlüsselungstechnologien spielt das Vertrauen zwischen den Kommunikationspartnern eine zentrale Rolle

Wer sensible Informationen austauscht, sollte seinen Datenverkehr durch Verschlüsselung wirksam vor unberechtigten Zugriffen schützen. Dabei muss natürlich sichergestellt sein, dass man sich auf alle involvierten Komponenten verlassen kann. Einen wichtigen Teil dieser Aufgabe leisten Vertrauensnetzwerke.

Es gibt immer mehr Branchen, in denen größere Unternehmen ihre kleineren Geschäftspartner anweisen, PKI-Zertifikate (PKI = Public-Key-Infrastruktur) für die Kommunikation und Authentifizierung einzusetzen. Auch per Gesetz oder im Rahmen elektronischer Ausschreibungsverfahren und nicht zuletzt bei der Kommunikation mit Behörden wird diese Technologie zunehmend verlangt. Es kann aber beileibe noch nicht davon gesprochen werden, dass die alltägliche geschäftliche Kommunikation zwischen Organisationen flächendeckend etwa mittels umfassender PKIs geschützt wird. Viele Unternehmer halten eine E-Mail-Verschlüsselung für viel zu kompliziert. Man hört sogar davon, dass die Verbreitung solcher Schutzmaßnahmen eher nachgelassen hat.

Schlüssel, Zertifikate und Dienste

Tatsächlich tun sich beim Einsatz von PKIs über Organisationsgrenzen hinweg einige Probleme auf. Doch zahlreiche Entwicklungen leisten hier Abhilfe. Schlüsselmaterial erhalten, den öffentlichen Schlüssel verfügbar machen und eigene Schlüssel verwalten, all das lässt sich heute ohne übermäßigen Aufwand bewältigen. Die Auswahl an Software und Zertifizierungsdienstleistern (Trust Service Provider, kurz: TSP) ist allerdings ziemlich unübersichtlich. Vor allem das Sicherheitsniveau fällt oft recht unterschiedlich aus. Es gibt z.B. kostenlose Zertifikate, bei denen gerade einmal die Existenz einer E-Mail-Adresse geprüft wird. Legt man also Wert auf eine nachgewiesene Organisationszugehörigkeit, sollte man sich für Zertifikate entscheiden, die höheren Richtlinien entsprechen.

Zudem muss sichergestellt sein, dass der private Schlüssel unter alleiniger Kontrolle des Benutzers (Eigentümer des Zertifikats) steht und niemals der erzeugenden und zertifizierenden Instanz zur Verfügung stand. Für das Verschlüsseln und die Prüfung der Signaturen ist ein Zugriff auf den öffentlichen Schlüssel dagegen notwendig. Potenzielle Kommunikationspartner müssen diesen dann auch über einen Verzeichnisdienst finden können. Alternativ ist natürlich ein manueller Austausch öffentlicher Zertifikate über signierte E-Mails ebenfalls denkbar.

Alle Partner der Kommunikationskette sollten diese verschiedenen Aspekte prüfen und bewerten. Für die Einrichtung und Pflege einer PKI kann so je nach Organisationsaufbau und eingesetzter Technologie mitunter einiger Aufwand anfallen. Um hierbei Hilfestellung zu leisten, beschäftigt sich TeleTrusT bereits seit 2001, gemeinsam mit Experten des vom Verband getragenen PKI-Vertrauensnetzwerkes TeleTrusT European Bridge CA (EBCA), mit diesen Fragen und empfiehlt folgende Maßnahmen:

Quelle: EBCA

Netzwerke schaffen Vertrauen beim Austausch von sensiblen Informationen.

Teil eines zentralen Vertrauensnetzwerkes werden

Erfüllt eine PKI bestimmte Mindestrichtlinien, kann man Vertrauensnetzwerke nutzen, die dem jeweiligen Partner die Beurteilung der Authentizität von Zertifikaten erleichtern. Ein Beispiel dafür ist das CA-Browser-Forum, das aufwendig bestimmt, welche Wurzelzertifikate in Browser-Zertifikatsspeichern abgelegt werden. Ein weiterer Ansatz besteht in Bridge CAs, die als Vertrauensvermittler die Bewertung von Zertifikaten vereinfachen. Sie arbeiten herstellerunabhängig und eignen sich daher besonders für Betreiber einer unternehmenseigenen PKI, also einem nicht-kommerziellen Trustcenter. Derzeit plant auch die Gesundheitsbranche im Rahmen der elektronischen Gesundheitskarte, ein solches Konzept umzusetzen. Die EBCA zählt ebenfalls zu diesen Initiativen.

Zertifikate leicht auffindbar hinterlegen

Nachdem eine Vertrauensbasis hergestellt ist, sollten die öffentlichen Schlüssel für potenzielle Interessenten verfügbar werden. Dazu können Unternehmen und Organisationen ihren Verzeichnisdienst öffentlich zugänglich machen. Damit auch alle Kommunikationspartner davon erfahren, gibt es bekannte Zugriffspunkte wie Proxies oder Gateways, über die Verzeichnisdienste gleich mehrerer Organisationen erreichbar sind. Häufig ist ein solcher Zugang bereits in der Verschlüsselungssoftware vorinstalliert. Natürlich muss dabei wiederum die Vertrauenswürdigkeit der angeschlossenen Partner gewährleistet sein. Die European Bridge CA stellt dies beispielsweise im Rahmen des EBCA-Verzeichnisdienstes sicher.

Die PKI pflegen und den Wissensaustausch vorantreiben

Sobald man Teil eines Vertrauensnetzwerkes und zum Beispiel über einen externen Verzeichnisdienst erreichbar ist, lassen sich etwaige Änderungen ohne große Mühe an einer zentralen Stelle durchführen. Auf diese Weise wird die Einrichtung und die Pflege der Public-Key-Infrastruktur wesentlich erleichtert.

Innerhalb des Vertrauensnetzwerkes sollte wenn möglich ein regelmäßiger und direkter Wissensaustausch mit anderen Nutzern und PKI-Experten der vernetzten Organisationen erfolgen. Denn allen aktuellen und zukünftigen Herausforderungen kann man gemeinsam am besten begegnen. Eine verbandsgestützte Initiative wie die European Bridge CA bietet auch hierfür eine stabile Plattform, die alle Mitglieder stets auf dem neuesten Stand hält und ihnen bei Problemen mit Rat und Tat zur Seite steht.

Fazit

Der praktische Nutzen eines Vertrauensnetzwerks hängt besonders im Umfeld von Public-Key-Infrastrukturen von seiner Größe und einer aktiven Mitarbeit aller Beteiligten ab. Denn je mehr Organisationen an PKI-Vertrauensnetzwerken wie der European Bridge CA teilnehmen und sich miteinander vernetzen, desto stärker wird die sichere Kommunikation zwischen den Organisationen gefördert. Und letztendlich lässt sich auf diese Art auch der Schutz sensibler Daten in der Gesellschaft allgemein stärken.

Marieke Petersohn
TeleTrusT – Bundesverband IT-Sicherheit e.V.

Impressum
Themenbeilage Sicherheit & Datenschutz

Redaktion just 4 business GmbH
Telefon: 08061 34811100, Fax: 08061 34811109,
E-Mail: tj@just4business.de

Verantwortliche Redakteure:
Thomas Jannot (v.i.S.d.P.), Martin Fuhrmann (Redaktion), Rudolph Schuster (Lektorat)

Autoren dieser Ausgabe:
Karsten U. Bartels, Prof. Dr. Christoph Busch, Hans-Joachim Giegerich, Dr. Christoph F-J Goetz, Peter Hansemann, Dr. Willi Kafitz, Dr. Gunnar Jacobson, Dr. Holger Mühlbauer, Marieke Petersohn, Dr. Burkhard Wiegel

DTP-Produktion:
Enrico Eisert, Kathleen Tiede, Matthias Timm, Hinstorff Verlag, Rostock

Korrektorat:
Kathleen Tiede, Hinstorff Verlag, Rostock

Titelbild:
© shutterstock, Max Griboedov; Collage: Matthias Timm, Hinstorff Verlag, Rostock

Verlag
Heise Medien GmbH & Co. KG,
Postfach 61 04 07, 30604 Hannover; Karl-Wiechert-Allee 10, 30625 Hannover;
Telefon: 0511 5352-0, Telefax: 0511 5352-129

Geschäftsführer:
Ansgar Heise, Dr. Alfons Schräder

Mitglied der Geschäftsleitung:
Beate Gerold

Verlagsleiter:
Dr. Alfons Schräder

Anzeigenleitung (verantwortlich für den Anzeigenteil):
Michael Hanke (-167), E-Mail: michael.hanke@heise.de, www.heise.de/mediadaten/ix

Leiter Vetrieb und Marketing:
André Lux

Druck:
Dierichs Druck + Media GmbH & Co. KG, Kassel

Die Inserenten

c’t Digitale Fotografie – die aktuelle Ausgabe 4/2015

Erfrischend anders!

Workshop mit Jana Mänz: Erfolgreich mit natürlichen Familienfotos

Foto: Jana Mänz

Kinder und Familien professionell portraitieren, die Bilder vermarkten und neue Aufträge bekommen – all das zeigt Ihnen der umfassende Workshop von Jana Mänz.
Wie Sie außerdem gezielt Farben einsetzen um Stimmungen zu erzeugen und Atmosphäre zu verstärken, demonstriert Ihnen Photoshop-Guru Pavel Kaplun.

Die neue Ausgabe 4/15 ist jetzt im Handel erhältlich oder digital im Google Play und Apple App Store oder für KindleFire.

Weitere Highlights der neuen Ausgabe:

- Mit Farbe bewusst gestalten
- 70–200mm Zooms im Test
- Autofokus perfektionieren
- SW-Fotos kolorieren

Tiefenschärfe mit Leidenschaft.

Bis 19. Juli versandkostenfrei für nur € 9,90 bestellen!

www.ct-digifoto.de