Besserer Vertraulichkeitsschutz in KMU durch Verschlüsselung

Tatjana Rubinstein · Mechthild Stöwer

Fraunhofer-Institut für Sichere Informationstechnologie
{tatjana.rubinstein | mechthild.stoewer}@sit.fraunhofer.de

Zusammenfassung

Der Schutz des Know-hows und die vertrauliche Handhabung von kritischen Mitarbeiter- und Kundeninformationen können zu einer Existenzfrage für KMU werden. Die Verschlüsselung von Informationen ist nach wie vor die bewährteste Technik, um Vertraulichkeit zu sichern. Die vorhandenen Verfahren zur Verschlüsselung gespeicherter („Data at Rest“) und übertragener Daten („Data in Transit“) werden von Unternehmen jedoch nur unzureichend genutzt. Insbesondere KMU tun sich sehr schwer, Konzepte zu entwickeln und zu implementieren. Dieser Beitrag stellt Ansatzpunkte für Verschlüsselungslösungen im Gesamtkontext dar, ordnet praktikable Lösungen den Anwendungsfeldern zu und gibt Empfehlungen für ein systematisches Vorgehen, um es KMUs zu erleichtern, eine auf ihre Belange zugeschnittene individuelle Verschlüsselungsarchitektur aufzubauen. Für die unter Vertraulichkeitsaspekten besonders kritische E-Mail-Kommunikation wird eine laientaugliche Lösung vorgestellt, die auch kleinen Unternehmen eine Ende-zu-Ende-Verschlüsselung erleichtert.

1 Problemaufriss

Innerhalb weniger Jahrzehnte ist Informations- und Kommunikationstechnik zur zentralen Ressource sowohl für die Prozesse innerhalb eines Unternehmens als auch für den Austausch mit Kunden, Dienstleistern, Kooperationspartnern, Aufsichtsbehörden und anderen öffentlichen und privaten Institutionen geworden. Dies ermöglicht völlig neuartige Anwendungen mit hoher Wertschöpfung, birgt gleichzeitig aber auch ebenso neuartige Risiken für das störungsfreie Funktionieren der kritischen Prozesse eines Unternehmens und die Vertraulichkeit der in und von ihnen gespeicherten, bearbeiteten und übertragenen Daten.

Mittelständische Unternehmen, die für den wirtschaftlichen Erfolg Deutschlands besonders wichtig sind, müssen das eigene Know-how und geistige Eigentum gut schützen, denn auch sie stehen im Fokus von Angreifern [CT14:8]. Die Verschlüsselung von Informationen ist das wirksamste technische Verfahren für diese Aufgabe. Obwohl seit Jahren bewährte Lösungen zur Verfügung stehen, werden diese oftmals nicht oder nur partiell genutzt [BSI11:58, 65], [kes12: 52ff]. Insbesondere E-Mails – auch mit vertraulichen Inhalten – werden nach wie vor in der Regel unverschlüsselt verschickt [BMWi12:24]. Ursachen hierfür sind mangelndes Bewusstsein über Bedrohungen und Auswirkungen der Verletzung des Vertraulichkeitsschutzes aber auch unzureichende Kenntnisse über die Funktionsweise von Verschlüsselung, mangelhafte Information über verfügbare Lösungen und deren Einsatz bei der Nutzung von Anwendungen. Hier helfen Sensibilisierung für Gefährdungen, Information über verfügbare Lösungen und deren zielgerichtete Nutzung und – natürlich – leichter zu benutzende Sicherheitslösungen [DsiN:15]. Aufgrund der Komplexität des Themas ist es insbesondere für KMU kein leichtes

P. Schartner · K. Lemke-Rust · M. Ullmann (Hrsg.) · D•A•CH Security 2015 · syssec (2015) 189-199.

Unterfangen, ein angemessenes Gesamtkonzept für die Anwendung von Verschlüsselung zu entwerfen, da diese sehr unterschiedliche Verfahren nutzt und ihr Einsatz prozessübergreifend geplant werden muss.

Zur Reduzierung der Komplexität könnte die Bereitstellung einer „laientaugliche“ Verschlüsselungslösung, die die Integration der kryptographischen Schlüssel in alle notwendigen Anwendungen des Nutzers automatisch vornimmt, die Verwendung einer sicheren Ende-zu-Ende Verschlüsselung sehr befördern. Ein solches System hat das Fraunhofer SIT mit der „Volksverschlüsselung“ entwickelt und unterstützt damit die breite Nutzung von Verschlüsselung.

2 Grundsätze des Vertraulichkeitsschutzes in KMU

Vor einer gezielten Planung des Einsatzes von Verschlüsselungslösungen sollten elementare Maßnahmen zum Schutz der Vertraulichkeit der Daten implementiert sein. Hierzu gehört insbesondere die Vergabe von Zugriffsrechten nach dem „Need to know“-Prinzip. Darüber hinaus sollte selbstverständlich sein, dass externe Schnittstellen des Unternehmensnetzes durch ein effektives Firewall-System gesichert sind, der Malwareschutz aktuell gehalten wird und sicherheitsrelevante Patches und Updates zeitnah installiert werden. Diese Maßnahmen müssen durch organisatorische Regelungen flankiert werden. Dies zielt insbesondere auf die Sensibilisierung der Mitarbeiter ab, die über einen sorgfältigen Umgang mit Daten informiert sein müssen. Hierzu müssen regelmäßige Unterweisungen stattfinden.

Die Nutzung von Verschlüsselungslösungen geht über diese Maßnahmen hinaus und bewirkt einen sehr effektiven Schutz von Informationen. Um solche Lösungen zu planen und gezielt einzusetzen, ist es wichtig, den Schutzbedarf der Daten und die Gefährdungen, denen diese an ihren Speicherorten und auf ihren Übertragungswegen ausgesetzt sind, einschätzen zu können. Dabei sollte ein besonderes Augenmerk auf solche Informationen gelegt werden, deren Geheimhaltung von besonders hoher, wenn nicht existenzieller Bedeutung für das Unternehmen ist. Dies können etwa personenbezogene Mitarbeiterdaten, die auch IT- und Netzwerkadministratoren verborgen bleiben müssen, vertrauliche Daten über die Verbindungen zu Geschäftspartnern und Kunden, Informationen zu Produktentwicklungen und Fertigungsverfahren oder Zugangsdaten zu Netzen und IT-Systemen sein. Insbesondere für solche Informationen ist ein systematisches Verschlüsselungskonzept zu entwickeln. Eine Richtlinie zur Informationsklassifizierung unterstützt die Durchsetzung dieses Konzepts.

Verschlüsselung kann auf unterschiedlichen Ebenen und für verschiedenste Anwendungen eingesetzt werden. Eine systematische Zusammenstellung ist hilfreich, die Möglichkeiten zum Einsatz dieser Technik für „Data at Rest“ und „Data in Transit“ auf allen Ebenen präsentiert.

Für „Data in Transit“ müssen Lösungen für unterschiedliche Kommunikationsanwendungen konzipiert und realisiert werden. Dies betrifft

- E-Mail-Kommunikation,
- Instant Messaging,
- Sprachkommunikation,
- Kollaborationsanwendungen und
- externe und ggf. interne Netzwerkzugriffe.

Gespeicherte Daten können verschlüsselt werden

- auf der Ebene der Datenträger,

- auf Ausschnitten von diesen (Containern- bzw. einzelnen Verzeichnissen) oder
- gezielt auf der Ebene einzelner Dateien.

Anhand dieser vielen Ansatzpunkte für Verschlüsselung wird deutlich, dass es nicht einfach ist, eine konsistente unternehmensweite Lösung zu finden, die den Anforderungen der Geschäftsprozesse gerecht wird, aber auch den langfristigen Zugang zu den Informationen sichert und einfach zu administrieren ist. KMU setzen oft auf Ad-hoc-Lösungen, die jedoch langfristig problembehaftet sind. So fehlt die Kontrolle über die Verteilung der Schlüssel, wenn Verschlüsselungsfunktionen von Anwendungsprogrammen wie MS Word oder Zip genutzt werden, oder aber ist der Zugriff auf verschlüsselte Verzeichnisse beim Ausscheiden von Mitarbeitern versperrt, wenn für solche Fälle erforderliche Wiederherstellungsverfahren nicht vorbereitet wurden [BSI08:8].

Viele Unternehmen nutzen bereits für einzelne Anwendungen Verschlüsselung. Sie verfügen jedoch über keine Strategie zur Weiterentwicklung dieser Ansätze hin zu einem systematisch gesteuerten Prozess. Reifegradmodelle können helfen, die Qualität einer Lösung einzuordnen und eine Perspektive für ein umfassendes Managementkonzept zu entwickeln. Hierzu gibt es Modelle, die in verschiedenen Stufen die Fähigkeit einer Institution zur zielgerichteten, effizienten und wirksamen Steuerung ihrer Abläufe beschreiben.

Abbildung 1 zeigt ein mehrstufiges Modell, das im Nachfolgenden erläutert wird.

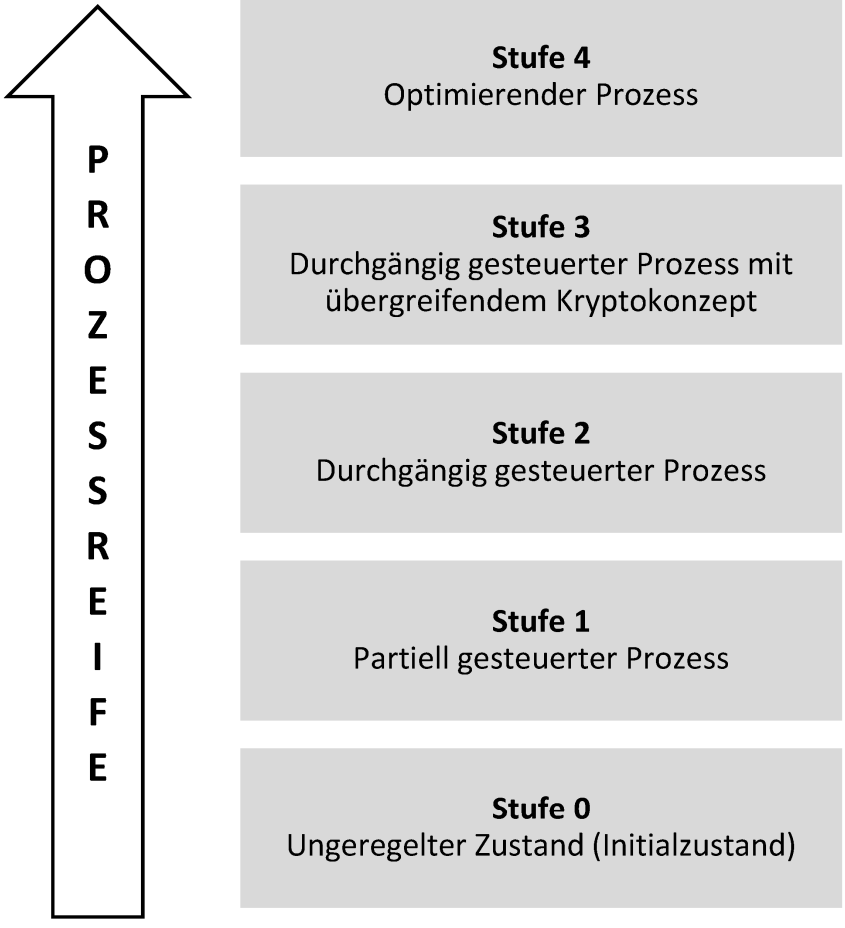

Abb. 1: Prozessreifegrade für Verschlüsselungslösungen

Stufe 0: Ungeregelter Zustand (Initialzustand)

Diesen Reifegrad erfüllt jede Organisation automatisch. Es gibt keine oder nur wenige organisatorischen Vorkehrungen und systematisch eingeführte technische Maßnahmen zum Vertraulichkeitsschutz durch Verschlüsselung. Diese Einstufung gilt – solange die betreffenden Aktivitäten nicht Teil einer Strategie oder der Richtlinien eines Unternehmens sind – auch dann, wenn beispielsweise einzelne Mitarbeiter in Eigeninitiative fallweise wichtige Dateien oder E-Mails verschlüsseln. Dieser Zustand ist charakteristisch für KMU, insbesondere das Fehlen einer Strategie und systematischer Planung.

Stufe 1: Partiell gesteuerter Prozess

Es gibt im Unternehmen vereinzelte Vorkehrungen und Regelungen zum Schutz vertraulicher Informationen, beispielsweise eine eingeführte Informationsklassifizierung, Software und Schlüssel zur Verschlüsselung von E-Mails oder Vorschriften zur Verschlüsselung der Festplatten mobiler IT-Systeme. Diese Maßnahmen sind aber nicht in ein Gesamtkonzept zum Schutz vertraulicher Informationen integriert. Für die Nutzung von Verschlüsselungstechniken sollte dies als Mindestmaß angestrebt werden, wobei das Fehlen einer Konzeption für den Vertraulichkeitsschutz auch für KMU eine gravierende Schwachstelle darstellt.

Stufe 2: Durchgängig gesteuerter Prozess

Es gibt ein Gesamtkonzept zum Schutz vertraulicher Informationen, das sicherstellen soll, dass vertrauliche Informationen auch als solche eingestuft und behandelt werden. Elemente dieses Gesamtkonzepts sind:

- eine Richtlinie zur Informationsklassifizierung, in der beschrieben ist, wie Informationen gemäß ihrer Vertraulichkeit eingestuft werden, wer diese Einstufung vorzunehmen hat und welche Konsequenzen sie für den Umgang mit den betreffenden Informationen hat,
- umfassende – also alle Speicherorte und Übertragungswege einschließende – Regelungen dazu, wie Informationen mit einem hohen und einem sehr hohen Grad an Vertraulichkeit durch Verschlüsselung geschützt werden sollen,
- eine Einbettung dieser Maßnahmen in ein übergreifendes Sicherheitskonzept des Unternehmens.

Es besteht aber noch ein Defizit hinsichtlich der Integration der kryptographischen Maßnahmen in ein explizites Kryptokonzept, in dem alle kryptographischen Maßnahmen untereinander abgestimmt sind. KMU sollten bestrebt sein, zumindest Stufe 2 für ihren Vertraulichkeitsschutz anzustreben.

Stufe 3: Durchgängig gesteuerter Prozess mit übergreifendem Kryptokonzept

Das Gesamtkonzept zum Schutz vertraulicher Informationen wird durch ein systematisches Kryptokonzept unterstützt, in dem unter anderem folgendes geregelt wird:

- ein durchgängiges Schlüsselmanagement (von der Erzeugung der Schlüssel bis hin zu deren Beseitigung),
- eine umfassende technische Unterstützung bei der Verwaltung der kryptographischen Instrumente und der Umsetzung von Sicherheitsrichtlinien zu deren Anwendung,
- das Zusammenwirken der zur Verschlüsselung eingesetzten kryptographischen Maßnahmen mit denen zur Integritätssicherung und Authentisierung,
- Recovery- und Notfallprozeduren.

KMU können diesen Reifegrad in der Regel mit eigenem Know-how nicht erreichen, ihn bei hohen Vertraulichkeitsanforderungen aber gleichwohl anstreben. In diesem Fall sollten sie daher die Hilfe externer Dienstleister in Anspruch nehmen, um fehlendes eigenes Know-how auszugleichen.

Stufe 4: Optimierender Prozess

In dieser Stufe wird über geeignete Instrumente regelmäßig überprüft, ob die Einzelmaßnahmen in den zuvor beschriebenen Konzepten wie gewünscht funktionieren und auch effizient (wirtschaftlich) sind.

Zur Messung der Prozessqualität und zur Identifikation von Verbesserungspotenzialen werden Kennzahlen aufgestellt, beispielsweise

- Anteil der klassifizierten Dokumente,
- Anteil der tatsächlich verschlüsselten vertraulichen Informationen,
- Anzahl korrumpierter Schlüssel, vergessener Passwörter oder anderer sicherheitsrelevanter Vorfälle im Zusammenhang mit den eingeführten kryptographischen Maßnahmen.

Durch geeignete Maßnahmen wird die kontinuierliche Verbesserung des Prozesses angestrebt. Es wird in regelmäßigen Audits geprüft, ob die Konzepte noch den Gegebenheiten entsprechen. Identifizierte Schwachstellen werden zeitnah behoben. Auch KMU sollten sich bemühen, durch geeignete Kennzahlen zu überprüfen, ob Maßnahmen zur Stärkung des Vertraulichkeitsschutzes wirken.

Insbesondere für kleine Unternehmen wird es in der Regel ausreichen, ein Gesamtkonzept zu entwickeln und dessen Funktionieren regelmäßig zu überprüfen. Sie sind überfordert, kryptographische Instrumente eigenständig zu verwalten und sie mit den Maßnahmen zur Integritätssicherung und Authentisierung zu verbinden. Best-Practice-Lösungen können helfen, gute Lösungen für diese Unternehmen zu finden. Die folgenden Vorschläge sollen als Muster für solche Referenzlösungen dienen.

3 Verschlüsselung in betrieblichen Prozessen

Um die Vertraulichkeit ihrer Daten angemessen zu sichern und bei der Nutzung von Verschlüsselung auch langfristig Zugriff auf die Daten zu haben, müssen KMU ein Vorgehensmodell entwickeln, das zumindest dem oben beschriebenen Reifegrad der Stufe 2 entspricht. Hierzu sind die folgenden Schritte auszuführen:

- Schritt 1: Bestimmung des Schutzbedarfs der genutzten Informationen,
- Schritt 2: Identifikation der Gefährdungen für Übertragungswege und Speicherorte vertraulicher Daten und Analyse ihrer Kritikalität,
- Schritt 3: Einführung angemessener Verschlüsselungslösungen für die Absicherung der vertraulichen Daten auf den kritischen Übertragungswegen und Speicherorten.

Folgendes Beispiel für ein kleines Handel- oder Handwerksunternehmen verdeutlicht die Umsetzung dieses Vorgehens (dieses und weitere Beispiele finden sich bei [KrWS15:51ff]).

Kennzeichnung des Anwendungsfalls

Bei dem Beispielunternehmen handelt es sich um einen kleinen Handels- oder Handwerksbetrieb, der inhabergeführt ist und rund zehn Mitarbeiter hat. Es gibt externe Kommunikationsbeziehungen über E-Mail etwa zu Lieferanten und Kunden. Hierzu werden Datenbestände wie

Adress-, Angebots- und Umsatzdaten verwaltet. Die Kunden des Unternehmens sind in der Regel Privatkunden oder aber andere kleine Unternehmen mit einfacher IT-Infrastruktur und entsprechend geringer IT-Kompetenz.

Die Finanzbuchhaltung wird intern erledigt, der Jahresabschluss erfolgt durch einen Steuerberater, der auch die Lohn- und Gehaltsbuchhaltung übernimmt.

Die IT-Infrastruktur ist nicht komplex. Es gibt drei PCs, einen davon mit Serverfunktion zur Ablage der Dateien und für die zentrale Datensicherung. Um bei Kundenbesuchen Informationen zu liefern und Angebote zu kalkulieren, gibt es einen Laptop, der aus der Ferne auch mit dem Firmennetz verbunden werden kann.

Das Unternehmen nutzt eine auf die Geschäftsanforderungen zugeschnittene Anwendungslösung und ein Finanzbuchhaltungsprogramm, für individuelle Korrespondenz und Kalkulationen gängige Office-Pakete.

Das Unternehmen wird von einem kleinen IT-Dienstleister betreut, der sowohl die Hardware als auch die Anwendungslösungen bereitstellt und konfiguriert. Kleine Anpassungen macht der Inhaber des Handwerksbetriebs selber, im Unternehmen sind jedoch keine explizite IT-Expertise und nur ein geringes Know-how zur IT-Sicherheit vorhanden.

Schritt 1: Bestimmung des Schutzbedarfs der Informationen

Tab. 1: Schutzbedarf der Informationen

Informationsbestände.	Bewertung
Personaldaten mit Gehaltsinformationen, Fehlzeiten etc.	Dies sind sehr sensible Informationen mit sehr hohen Vertraulichkeitsanforderungen.
Kundendaten (Adressen, Angebote, erbrachte Leistungen und Umsätze)	Dies sind sensible Informationen mit hohen Vertraulichkeitsanforderungen.
Leistungsverzeichnisse	Diese Informationen haben geringe Vertraulichkeitsanforderungen, da sie z. T. öffentlich verfügbar sind. Dort, wo sie unternehmensspezifisch sind, würde bei unberechtigten Zugriffen kein Schaden entstehen.
Lagerinformationen	Dies sind für das Unternehmen sensible Informationen. Die Vertraulichkeitsanforderungen sind hoch, da diese Informationen das Know-how der Firma repräsentieren und einen Konkurrenzvorteil bieten können.
Kalkulationen	Dies sind sehr sensible Informationen. Die Vertraulichkeitsanforderungen sind sehr hoch.

Schritt 2: Bestimmung der Gefährdungen und der Kritikalität von Übertragungswegen und Speicherorten

Ein solches Unternehmen stellt in der Regel kein spezifisch attraktives und exponiertes Angriffsziel dar. Die Gefahr, gezielt angegriffen zu werden, ist gering. Trotz allem kann das Unternehmen von breit gestreuten Attacken betroffen sein.

- Es kann zu Vertraulichkeitsverletzungen durch Zugriff auf Datenträger beim Verlust von mobilen Geräten kommen. Kundendaten und Kalkulationen könnten nicht berechtigten Personen (z. B. Konkurrenzunternehmen) zugänglich werden.
- Auf den Arbeitsplatzrechnern könnten nicht Berechtigte auf Informationen über Mitarbeiter, Kunden, Kalkulationen und Finanzen zugreifen. So könnten etwa unzufriedene

Mitarbeiter Kundendaten abgreifen, um sie beim Ausscheiden mit in eine neue Firma zu nehmen.

- Der unberechtigte Zugriff auf personenbezogene Daten kann zu Datenschutzverletzungen mit strafrechtlichen Konsequenzen führen.
- Bei der Übertragung von Informationen, z. B. bei der E-Mail-Kommunikation mit Kunden über Angebote und der Bereitstellung von Informationen für den Steuerberater, sind unberechtigte Zugriffe auf schutzbedürftige Daten möglich.

Obwohl die Gefahr gezielter Hackerangriffe von außen vergleichsweise gering ist, hat das Unternehmen daher Anforderungen an die Vertraulichkeit seiner Daten und damit einen Bedarf, diese zu schützen.

Schritt 3: Skizze einer Lösung

Das Handwerksunternehmen sollte für kritische Daten Verschlüsselungslösungen wählen. Eventuell sollte das Unternehmen seinen IT-Dienstleister ansprechen und Unterstützung für die Planung und Umsetzung von Lösungen nutzen.

Übertragung von Informationen – Data in Transit

- Werden personenbezogene oder buchhalterische Daten per E-Mail (etwa an den Steuerberater) übertragen, sind diese zu verschlüsseln. Sind die Anhänge mit einem Office-Programm verschlüsselt, muss der Kommunikationspartner den Schlüssel kennen. Er könnte etwa in einem Telefonat mitgeteilt werden. Die E-Mail selber ist dann jedoch noch nicht verschlüsselt. Hierzu könnte die vom Fraunhofer SIT entwickelte Volksverschlüsselung genutzt werden (siehe Abschnitt 4). Dies ist auch eine einfach zu nutzende Option für Kommunikationspartner wie den Steuerberater.
- Auch ein verschlüsselter Datenaustausch mit Kunden ist über die Nutzung der Volksverschlüsselung möglich und sollte vom Unternehmen angeboten werden.

Verschlüsselung gespeicherter Informationen – Data at Rest

- Besonders kritisch ist der Einsatz eines Laptops für Arbeiten bei den Kunden. Um unberechtigte Zugriffe auf schutzwürdige Informationen zu erschweren, sollten die Datenbestände auf diesem Gerät grundsätzlich regelmäßig daraufhin überprüft werden, ob sie für den mobilen Einsatz benötigt werden. Es sollten nur wirklich erforderliche Firmendaten auf der Festplatte des Geräts abgelegt sein.
- Darüber hinaus sind die Informationen auf dem Gerät durch eine Festplattenverschlüsselung zu schützen, ebenso wie ein eventuell genutzter USB-Stick eine Hardwareverschlüsselung besitzen sollte. Die verwendeten Kennwörter und Wiederherstellungsschlüssel sind sicher zu hinterlegen, damit sie im Notfall verfügbar sind.
- Auch die Informationsbestände auf den Arbeitsplatzrechnern sollten durch eine angemessene Verschlüsselung geschützt werden. Die bei dem Unternehmen genutzten Branchenlösungen bieten in der Regel keine Verschlüsselungsmöglichkeiten für Datenbestände. Daher ist es sinnvoll, die Anwendungen und die von ihnen genutzten Dateien in verschlüsselten Containern auf der Festplatte des Arbeitsplatzrechners abzulegen. Dies gilt insbesondere für sensible personenbezogene Daten, die dadurch dem Zugriff Unberechtigter entzogen sind. Für die Erzeugung der hierfür nötigen Schlüssel kann ebenfalls die oben genannte Volksverschlüsselung dienen.

Diese drei Schritte sollten KMU durchlaufen und entsprechend der Kritikalität der Daten konsistente Verschlüsselungslösungen nutzen.

4 Vorstellung einer Verschlüsselungslösung

E-Mail ist zum wichtigsten Kommunikationsmedium geworden – auch in KMU und auch hier für vertrauliche Inhalte. Aber nach wie vor wird nur ein geringer Anteil der E-Mails verschlüsselt. So nutzen nur wenige KMU frei verfügbare Lösungen wie PGP oder bauen eigene S/MIME-basierte PKIs als Basis für vertrauliche E-Mail auf.

Die zurückhaltende Anwendung einer wirksamen Ende-zu-Ende-Verschlüsselung hat eine Vielzahl an Ursachen [Herf13:7ff]:

- Anwendern stehen keine kryptographischen Schlüssel zur Verfügung. Selbst engagierte Nutzer haben keine Institution, die ihnen vertrauenswürdiges Schlüsselmaterial zur E-Mail-Verschlüsselung bereitstellt.
- Anwender nutzen eine Vielfalt von Lösungen für die E-Mail Kommunikation (etwa MS Outlook, Thunderbird oder diverse Web-Mail-Portale), die keine standardisierten Schnittstellen und Architekturkonzepte nutzen. Die meisten Nutzer haben keine Expertise, wie sie diese Anwendungen richtig und sicher für eine Verschlüsselung konfigurieren können.
- Um mit Partnern verschlüsselt zu kommunizieren, braucht ein Sender den öffentlichen Schlüssel des Empfängers. Es fehlt aktuell an einer Infrastruktur, um Schlüssel breit verfügbar zu machen.
- Das Konzept der Nutzung eines Schlüsselpaars für eine asymmetrische Verschlüsselung ist nicht intuitiv nachvollziehbar und daher für einen nicht technisch orientierten Nutzer nur schwer verständlich.

Aufgrund dieser Komplexität sind private Anwender, aber auch KMU kaum in der Lage, E-Mail-Verschlüsselung einzusetzen. An diesen Problemen setzt die vom Fraunhofer-Institut für Sichere Informationstechnologie entwickelte Volksverschlüsselung an. Diese Lösung bietet eine Infrastruktur für eine „laientaugliche“ Verschlüsselung.

Das wesentliche Element ist eine Client-Komponente (VV-Software), die gemäß dem Prinzip „Usability by Design“ entwickelt wird und für deren Anwendung auch Laien keine Anleitung benötigen. Diese Anwendung wird auf dem Rechner des Benutzers installiert und erledigt automatisch auf sehr einfache Weise alle erforderlichen Schritte, damit auch ein ungeübter Benutzer verschlüsselt per E-Mail kommunizieren kann. Abbildung 2 zeigt die Leistungsmerkmale und Abläufe der Volksverschlüsselung.

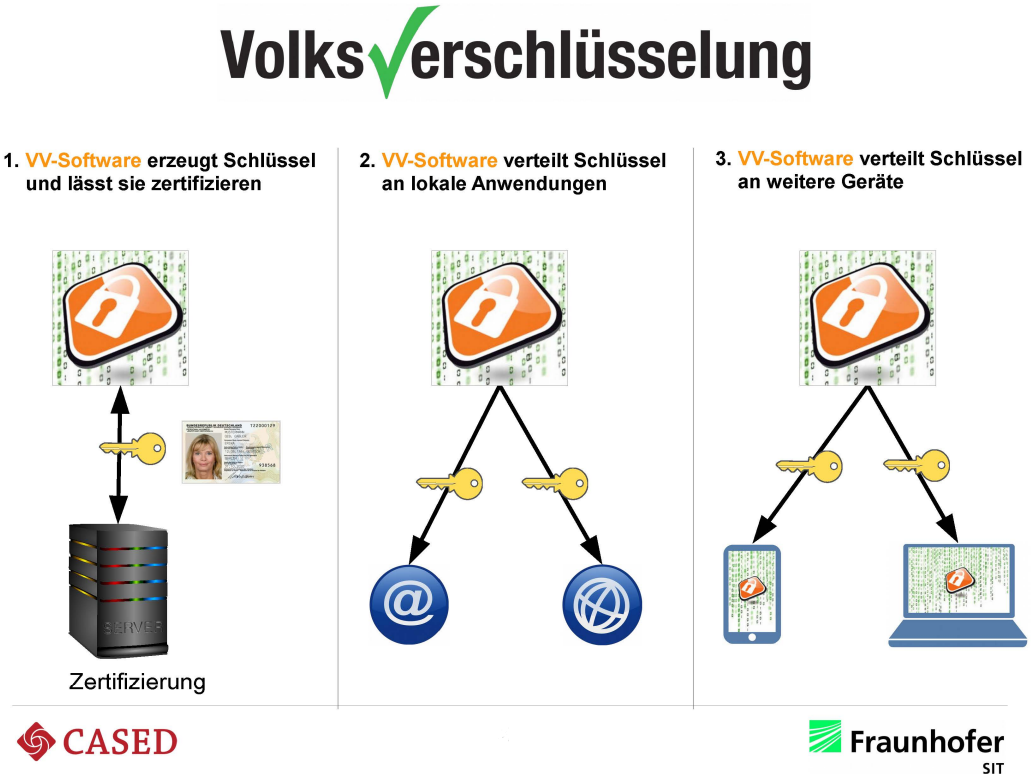

Abb. 2: Leistungsmerkmale und Abläufe der Volksverschlüsselung

1. Nach Prüfung der E-Mail-Adresse und der Identität des Benutzers erzeugt die Anwendung kryptographische Schlüssel (siehe Abbildung 3):
   - Zur Identitätsprüfung wird durch die Nutzung des neuen Personalausweises ein sicheres und verfügbares Verfahren verwendet. Aus dem Personalausweis werden lediglich der Vorname, Name und ggf. der akademischer Titel ausgelesen und für die Zertifikate verwendet. Zusätzlich wird die eingerichtete E-Mail-Adresse des Nutzers verwendet.
   - Weitere Identifizierungsverfahren werden hinsichtlich ihrer Sicherheit und Tauglichkeit geprüft, darunter auch das Postident-Verfahren.
   - Automatisch werden die öffentlichen Anteile von einem bei einer vertrauenswürdigen Einrichtung betriebenen zentralen Server als Klasse 3-Zertifikate zertifiziert. Der private Schlüssel verbleibt zu jedem Zeitpunkt beim Benutzer. Der Server erzeugt drei unterschiedliche Zertifikate für Verschlüsselung, Authentisierung und Signatur.
2. Die Anwendung steuert die Integration der Schlüssel und der Zertifikate in das E-Mail-Programm, den Browser und andere kryptographischer Anwendungen des Rechners, auf dem sie installiert ist. In der aktuellen Version werden MS Outlook, Internet Explorer, Chrome, Firefox und Thunderbird unterstützt. Die Anwendung unterstützt den Benutzer während des gesamten Gültigkeitszeitraums des Zertifikats, etwa durch eine rechtzeitige Information über dessen Ablauf des Zertifikat oder falls für die Verschlüsselung vorgesehene kryptographische Verfahren nicht mehr als sicher gelten.
3. Darüber hinaus können auf einfache Weise von dort aus Schlüssel und Zertifikate in Smartphones, Tablets und weitere Geräte des Benutzers übertragen und dort installiert werden.

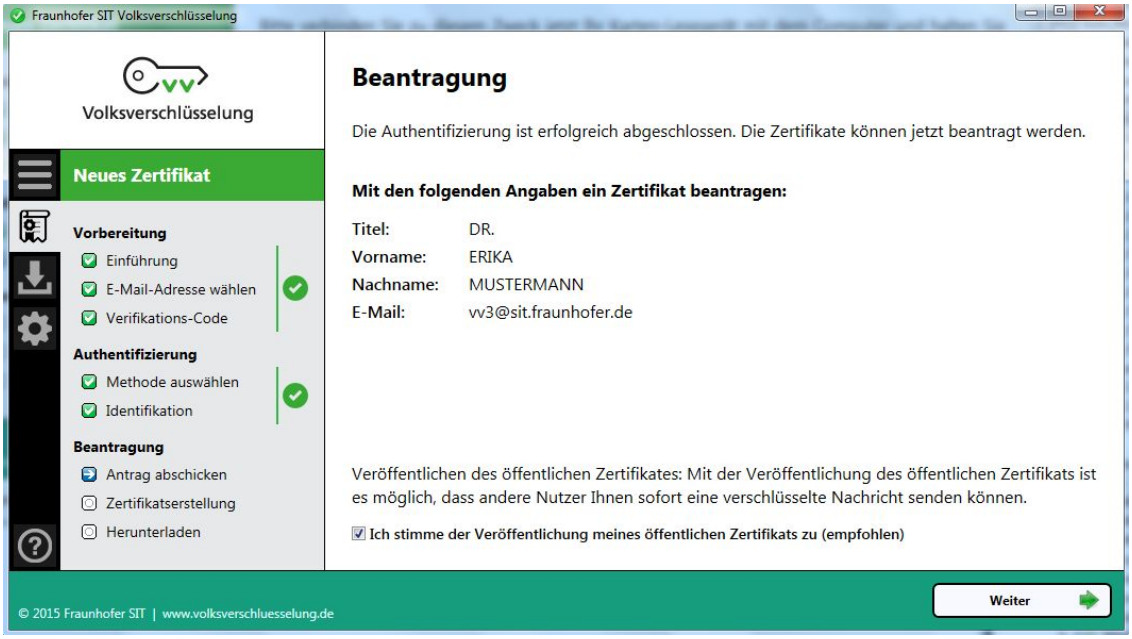

Abb. 3: Beantragung eines Zertifikats

Die Erstellung und Verwaltung der Zertifikate übernimmt eine hochsichere PKI. Über eine TLS/SSL-geschützte REST-Schnittstelle werden Anträge an die RA (Registration Authority) übertragen. Für die Implementierung der CA (Certification Authority) wird die Open-Source-Software EJBCA genutzt, über die auch weitere Funktionen wie das Management von Sperrlisten oder der OCSP-Dienst organisiert sind. Ein Verzeichnisdienst veröffentlicht die Zertifikate (falls vom Benutzer ausdrücklich erwünscht) und stellt sie Kommunikationspartnern zu Verfügung.

So wird kleinen Unternehmen, die über kein explizites Know-how zu Verschlüsselung, Signatur und Authentisierung verfügen, eine einfach zu nutzende Infrastruktur zur Verfügung gestellt, die eine sehr hohe Vertraulichkeit in der Kommunikation sowie eine hohe Authentizität in der Verwendung von Webdiensten bietet.

Diese Infrastruktur ist sehr flexibel. Unternehmen, die eine eigene PKI betreiben wollen, können sowohl die zentralen Komponenten als auch die Client-Komponente der Lösung leicht in die bei ihnen vorhandene Infrastruktur integrieren und für ihre Verschlüsselungsanwendungen nutzen. Auch die nPA-Identifizierungskomponente in der VV-Software ist modular aufgebaut und kann durch ein anderes Verfahren ersetzt werden, z. B. durch Postident oder andere landesspezifische eID-Systeme.

5 Ausblick

Trotz der großen Gefahr durch Wirtschaftsspionage oder andere Bedrohungen für die Vertraulichkeit sensibler Daten nutzen insbesondere KMU Möglichkeiten zur Verschlüsselung ihrer Daten nur unzureichend. Hauptursache hierfür ist, dass ihnen gut aufbereitete Informationen und leicht zu nutzende Lösungen zur Anwendung von Verschlüsselung fehlen. Best-Practice-Beispiele können ihnen einen Weg weisen bei der Bewertung der Kritikalität ihre Daten und der Anwendung geeigneter Verschlüsselungslösungen. Für E-Mail steht eine neue Infrastruktur bereit, die Anwender mit zertifizierten Schlüsseln versorgt und ihnen durch eine Client-Anwendung eine „laientaugliche“ Installation und Benutzung dieser Schlüssel für eine verschlüsselte

E-Mail-Kommunikation bietet. Dies ist ein wesentlicher Baustein für den Schutz des Know-hows und anderer sensibler Daten eines Unternehmens.

Literatur

[BSI08] Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): Leitfaden Erstellung von Kryptokonzepten (2008) www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Kryptokonzept_pdf.html.

[BSI11] Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): Studie zur IT-Sicherheit in kleinen und mittleren Unternehmen (2011) www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/KMU/Studie_IT-Sicherheit_KMU.pdf?__blob=publicationFile.

[BMWi12] Bundesministerium für Wirtschaft und Technologie (Hrsg.): IT-Sicherheitsniveau in kleinen und mittleren Unternehmen (2012), www.bmwi.de/BMWi/Redaktion/PDF/S-T/studie-it-sicherheit.pdf.

[CT14] Corporate Trust: Studie Industriespionage (2014) www.corporate-trust.de/pdf/CT-Studie-2014_DE.pdf.

[DsiN] Deutschland sicher im Netz e.V.: Leitfaden Verschlüsselung von E-Mails, www.sicher-im-netz.de/sites/default/files/download/leitfaden-e-mail-verschluesselung.pdf.

[Herf13] M. Herfert et al.: Privatsphärenschutz und Vertraulichkeit im Internet, Darmstadt (2014), www.sit.fraunhofer.de/fileadmin/dokumente/studien_und_technical_reports/TuS-Bericht_Privacy.pdf.

[kes12] P. Hohl (Hrsg.): <kes> – Die Zeitschrift für Informations-Sicherheit, Lagebericht zur Informationssicherheit (3), Nr. 6/2012.

[KrWS15] R. Kraft, F. Weber, R. Marx, M. Stöwer, H. Große-Onnebrink, P. Larbig, A. Oberle: Vertraulichkeitsschutz durch Verschlüsselung, Strategien und Lösungen für Unternehmen, Darmstadt (2015).