Zentral definierte Verschlüsselung

Daten sicher transportieren

Der Schutz firmeneigener Information auf dem Transportweg berührt ein Spannungsfeld der IT: Der Benutzer kann zwar die Sensibilität der jeweiligen Information selbst am besten einschätzen, hat aber weder Expertise im Umgang mit Verschlüsselungstechnik noch Zeit für eine „Sonderbehandlung" der Information nach zentral definierten Regeln.

Produkte, die das zentrale, netzweite Management der Vertraulichkeit bei gleichzeitig einfacher Nutzbarkeit und geeigneter Individualisierung an die Unternehmensrichtlinien verbinden, entschärfen das Problem der mangelnden Erfahrung von Anwendern mit Kryptosoftware. Etablierte Lösungen zur Verschlüsselung für unterwegs, wie sie beispielsweise Utimaco mit Safe Guard Easy sowie Pointsec oder Safe Boot seit längerem in Form einer Partitionsverschlüsselung mithilfe eines Firmenschlüssels geliefert werden, werden nicht jeder Umgebung gerecht. Es gibt Anwendungsfälle, bei denen eine andere Technik mehr Erfolg verspricht.

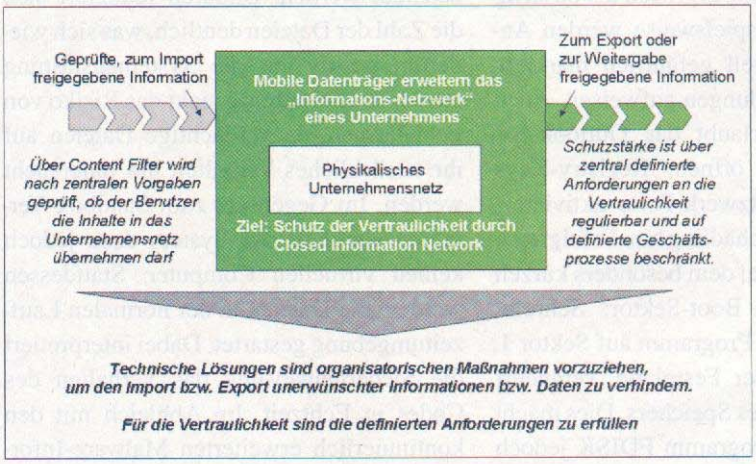
Anwendungsfall „Mobility": Vertriebsmitarbeiter möchten sensible Kundendaten zum Kunden transportieren und dort auf ihren Memory Sticks oder anderen Datenträgern übergeben, ohne dass bei Verlust oder Diebstahl des Datenträgers ein Sicherheitsrisiko für die Daten besteht. Natürlich darf der Vertriebsmitarbeiter den geheimen Unternehmensschlüssel – sofern er ihn überhaupt kennt – nicht weitergeben und auch nicht auf fremden Systemen hinterlassen, da beispielsweise die Schlüsseleingabe auf. Folglich benötigt besagter Vertriebsmitarbeiter jeweils kundenspezifische Schlüssel. Diese Anforderung könnte natürlich grundsätzlich durch eine vorkonfektionierte PKI oder Produkte mit benutzerseitiger Schlüsseleingabe erfüllt werden. Eine PKI scheidet jedoch in diesem Szenario oft aus

Die Produkte zur Schlüsseleingabe verlangen vor der Auslagerung der Daten eine Benutzeraktion – je nach Qualität kann der Benutzer etwa durch eine Aktion im Kontextmenü (rechte Maustaste) die Verschlüsselung aktiv anfordern. Diese Aktion erfordert aber neben der „Awareness" des Nutzers auch Zeit und und Geduld. Schließlich stellt der Umstand, dass pro Datenträger bei Partitionsverschlüsselung nur ein Schlüssel verwendet werden kann, ein weiteres Problem dar.

Anwendungsfall „Multi Key": Zusätzlich zu der eben beschriebenen Anforderung möchte der Vertriebsmitarbeiter auf seinem persönlichen Memory Stick möglichst alle Kundendaten unterbringen. Für einen einzelnen Kunden will er allerdings nur die für ihn bestimmten Daten offen legen – unabhängig davon, ob er den Schlüssel und den Datenträger direkt weitergibt oder durch Eingabe eines kundenspezifischen Schlüssels auf einem unsicheren, weil fremden Rechner diesen Datenträger selbst entschlüsselt. Diese Anforderung kann durch Lösungen, welche nur einen einzigen Schlüssel für die gesamte Partition vorsehen – so etwa durch eine PIN-Eingabe für selbst verschlüsselnde Memory Sticks mit hohem Schutzgrad, erhältlich beim Anbieter Kobil – nicht erfüllt werden.

Die Anforderung der „Usability", das heißt der einfachen Nutzbarkeit, wurde hier bereits erwähnt. Welche konkreten Anforderungen resultieren daraus? Zunächst darf dem Benutzer nicht allzu viel planende Tätigkeit zugemutet werden, sondern alle Aktivitäten und Entscheidungen des Benutzers sollten voll automatisiert in die Standardprozesse integriert sein. Da es im beschriebenen Fall um die Vertraulichkeit während des Transportes geht, sind die Auslagerung aus einer sicheren Umgebung (Export) und das Einlesen in eine geschützte Umgebung (Import) zu unterscheiden. In beiden Situationen ist es wesentlich, dass Zugriff aufs Schlüsselmaterial besteht. Erfahrungsgemäß ist hier der Kopf des Mitarbeiters nach wie vor der beste Aufbewahrungsort, da er sich natürlicherweise stets am Ort des Geschehens befindet.

Escrow-Anforderungen (Bereithaltung des Schlüssels für berechtigte Zugriffe durch andere Personen als den Endanwender) bestehen nicht, denn bei einem vertraulichen Transport von Daten bleiben die Originale in der jeweils sicheren Umgebung unverändert erhalten; der Mitarbeiter nimmt ledig-



Sytematische, zentral verwaltete Verschlüsselung entlastet die Anwender
Quelle: Sios

lich Kopien mit. Von Datenveränderungen direkt auf den mobilen Datenträgern ist abzuraten, da bereits ein kurzer Kontaktausfall zum speichernden Gerät den Verlust der Originaldaten bedeutet – Ausnahmen stellen hier U3-Lösungen dar, die aber derzeit noch kaum verbreitet sind. Aus diesem Grund sind auch Lösungen mit Vorsicht einzusetzen, die das Löschen des Originals als Option anbieten und dann nur eine verschlüsselte Version auf einem mobilen Datenträger übriglassen.

Anwendungsfall „Datenexport“: Für den Datenexport muss unabhängig vom verwendeten Verfahren in der Microsoft-Umgebung (Drag and Drop, Cut and Paste oder Kontextmenü) eine Benutzerführung mit wenigen, einleuchtenden Schritten in die Standardprozesse integriert sein. Sicherheitsregeln dürfen nicht umgangen werden.

Anwendungsfall „Datenimport“: Auf Zielsystemen darf keine Installation erforderlich sein, da viele Anwender nicht zur Installation berechtigt sind. Das Entschlüsselungswerkzeug muss beim Verschlüsseln automatisch auf jeden Datenträger kopiert werden.

„Zielabhängige Wahl der Verschlüsselung“ und „inhaltsabhängige Wahl der Verschlüsselung“: Es gibt in jedem Unternehmen Daten, die unkompliziert und ohne Vertraulichkeitsanforderung kommuniziert werden können. Zum Beispiel sind Firmenbroschüren, Produktbeschreibungen und andere öffentlich zugängliche Informationen die Basisausstattung jedes Vertriebsmitarbeiters. Wie immer ist hier die richtige Dosierung der Sicherheit von zentraler Bedeutung, um einen „Verschleiß des Sicherheitsbewusstseins“ zu verhindern. Deshalb ist es sinnvoll, auf Datenträgern wie etwa Memory Sticks oder mehrfach beschreibbaren CDs oder DVDs auch unverschlüsselte Daten zuzulassen. Bei der Auslagerung von Bilddaten auf digitale Fotoapparate, Bilddrucker oder andere Geräte ist eine Verschlüsselung sogar unbedingt zu verhindern, da sonst das Gerät nicht arbeiten kann. Die Verschlüsselung ist also durch eine zentrale Vorgabe je nach Zielgerät zu steuern. Dabei ist durch eine geeignete inhaltliche Kontrolle der Dateien und nicht nur der Dateinamen sicher zu stellen, dass keine umbenannten, sensiblen Inhalte das Firmennetz unverschlüsselt verlassen.

Die Entscheidung, welche Daten zur Verschlüsselung anstehen, ist deshalb nicht nur vom Ziel der Kopieroperation, sondern stets auch vom Inhalt abhängig zu machen. Sie kann sich nicht auf Dateitypen stützen, sondern muss die Möglichkeit inhaltliche Prüfungen (Content- und Pattern-Scanning) einbeziehen. Je nach Firmenrichtlinie wird prinzipiell alles verschlüsselt, und nur speziell definierte Dateien können unverschlüsselt ausgetauscht werden (White List Policy), oder es ist grundsätzlich alles unverschlüsselt und nur besondere Daten werden zwangsweiser Verschlüsselung unterworfen (Black List Policy).

Sind all diese Anforderungen erfüllt, können Unternehmen auch „exotische“ Anforderungen zentral verwalten und netzwerkweit durchsetzen. So kann beispielsweise beim Itwatch-Produkt „Pdwatch“ in Kombination mit dem Content-Prüfer „Xraywatch“ definiert werden, dass Word-Dokumente mit dem in der Fußzeile befindlichen Zusatz „firmenvertraulich“ zu verschlüsseln sind. Ein Anwenderbericht zu einem entsprechenden Gebrauch von Content-Filtern wurde auf der Microsoft-Polizeikonferenz vorgestellt [2].

Produkte mit den beschriebenen Eigenschaften halten sich an die zeitgemäße IT-Manager-Philosophie: „Nicht gängeln, sondern unterstützen“, und zwar durch die automatisierte Integration in Windows für alle Anwendergruppen. Technische Kenntnisse oder spezielle Awareness müssen beim Anwender nicht vorausgesetzt werden. So kann der Datenschutzbeauftragte oder Information Security Officer eines Unternehmens etwa mit einer einfachen, im Produkt enthaltenen Policy die Verschlüsselung bei der Auslagerung anfordern. Falls einem Benutzer ein Recht für das unverschlüsselte Auslagern zugesprochen wird, geht die Verantwortung auf den Benutzer über, der durch eine persönliche Aktion seine Zustimmung zur unverschlüsselten Auslagerung im Einzelfall bestätigt.

Dr. Peter Scholz/wj

Anforderungen an die Vertraulichkeit beim Datentransport

1. Verschlüsselung mit verschiedenen Schlüsseln auf einem Datenträger
   a. Im Bedarfsfall werden die Schlüssel durch den Benutzer gewählt
   b. Unverschlüsselte Dateien liegen neben verschlüsselten auf einem Datenträger
2. Zentrale Definition der Schlüsselstärke, eventuell der Verschlüsselungsverfahren und Richtlinien
   a. Wer darf unverschlüsselt auslagern?
   b. Die Schlüsseleigenschaften eines starken Schlüssels sind zentral zu definieren.
   c. Welche Dateien/Contents dürfen unverschlüsselt ausgelagert werden?
   d. Auf welche Geräte/Devices darf unverschlüsselt ausgelagert werden – für welche wird eine Verschlüsselung erzwungen?
   e. Unterliegt die Weitergabe einer Protokollierung oder einem Shadowing?
3. Vollautomatisierte Integration in Windows: Alle Standard Windows Mechanismen für das Dateimanagement müssen automatisch in die Verschlüsselung münden.
   a. Verschlüsselung per Drag and Drop
   b. Verschlüsselung per Cut and Paste
   c. Kontext-Menüoperationen (Kopieren und Einfügen)
4. Keine Umgehung der Sicherheitseinstellungen für sensible Daten
5. Entschlüsselungssoftware muss automatisch mitgeliefert werden und darf keine Installation im Zielsystem erfordern.

Quellenangaben

[1] Peter Scholz: Unbekannte Schwachstellen in Hardware und Betriebssystemen. Handbuch der Telekommunikation, Wolters Kluwer Verlag, März 2005.
[2] Digitale Fotografie auf dem XP-Arbeitsplatz der Bayerischen Polizei, Erfahrungen im Zusammenhang mit der Einführung eines fachspezifischen Polizeiarbeitsplatzes und im Umgang mit Bilddaten, PP Oberbayern und PP Niederbayern Oberpfalz, 11. Microsoft-Polizeikongress 3./4. April 2006 in Bad Homburg

Dr. Peter Scholz arbeitet für Sios in München.